COMS3000/7003

Information Security

Adjunct A/Prof David Ross

dross@itee.uq.edu.au

David.Ross.3@team.telstra.com

Welcome to Information Security COMS3000/7003

- Today's Lecture:
  - Administrative details
  - Course Content
  - Lectures, Tutorials, Assignments
  - Assessment, Marking

  - Security Introduction
  - Risk Management

BTW, please ask questions any time!

Teaching Staff

- Adjunct A/Prof David Ross (Course Coordinator, Lecturer)
  - Email: dross@itee.uq.edu.au
  - Email: David.Ross.3@team.telstra.com
  - Office: 78-304 (Fridays ONLY)
  - Office: 275 George Street, Brisbane (all other times)
  - Phone: 0439 404 637
  - Consultation time: on request
    - Just send me an email

- Tutors:

Mr Kristan Edwards	<kristan.edwards@uq.edu.au>
Dr Kaleb Leemaqz	<k.leemaqz@uq.edu.au>

Lecturer

- Dr David Ross (Course Coordinator, Lecturer)
  - Managing Consultant (IT Security Consultant), Telstra
  - Chartered Professional Engineer (Electrical) (CPEng)
  - Registered Professional Engineer – Queensland (RPEQ)
  - Certified Information Systems Security Professional (CISSP)
  - Global Industrial Cyber Security Professional (GICSP)
  - PCI DSS Qualified Security Assessor (PCI QSA)
  - Payment Card Industry Professional (PCIP)
  - Founding Director, Cloud Security Alliance Australia Chapter
  - Standards Australia IT-012-04 (Information Security) Committee
  - Standards Australia IT-038 (Cloud Computing) Committee
  - SABSA Chartered Foundation (SCF) Certificate
  - SABSA Chartered Practitioner: Architectural Design (SCPA)
  - PhD in Wireless Network Security

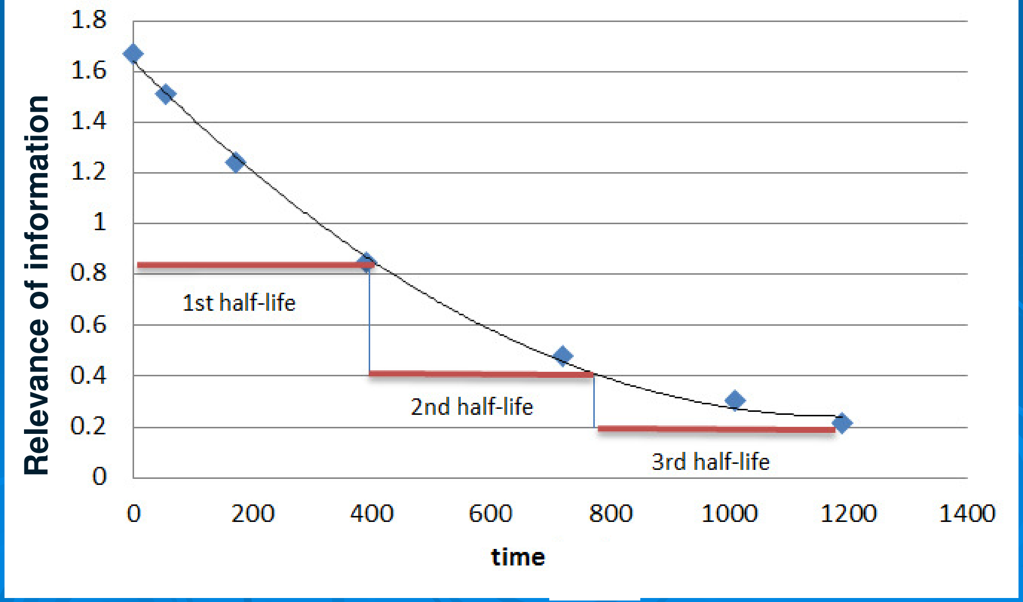
Course Content

(subject to small changes)

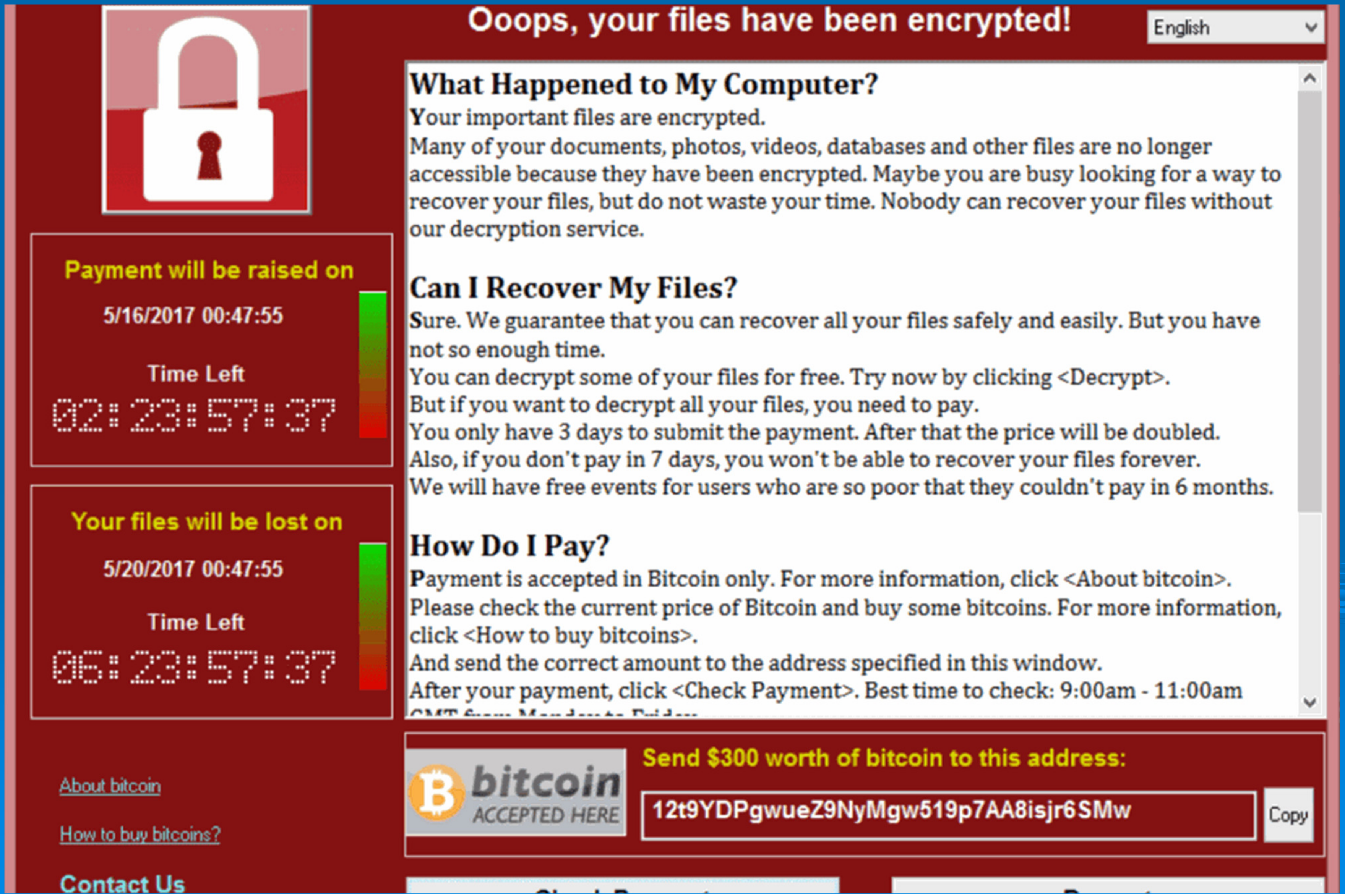
- Risk Management
- Authentication
- Authorisation
- Access Control
- Information Theory
- Cryptography
  - Secret-key
  - Public-key
- Network Security, Protocols
- Payment Card Industry (PCI) Security
- Cloud Computing Security
- Industrial Control Systems (ICS) Security

Course Focus

- Basic Information Security concepts
  - Not how to use the latest version of Metasploit, Nessus, Nmap, etc.
- Generally, focus more on information with a longer "half-life".
- What's "half-life"?
  - The amount of time required to halve a given metric
  - Half-life is constant for exponential decay, e.g. radio active decay
  - Sometimes used informally to discuss decay of relevance of information



Security in the News



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

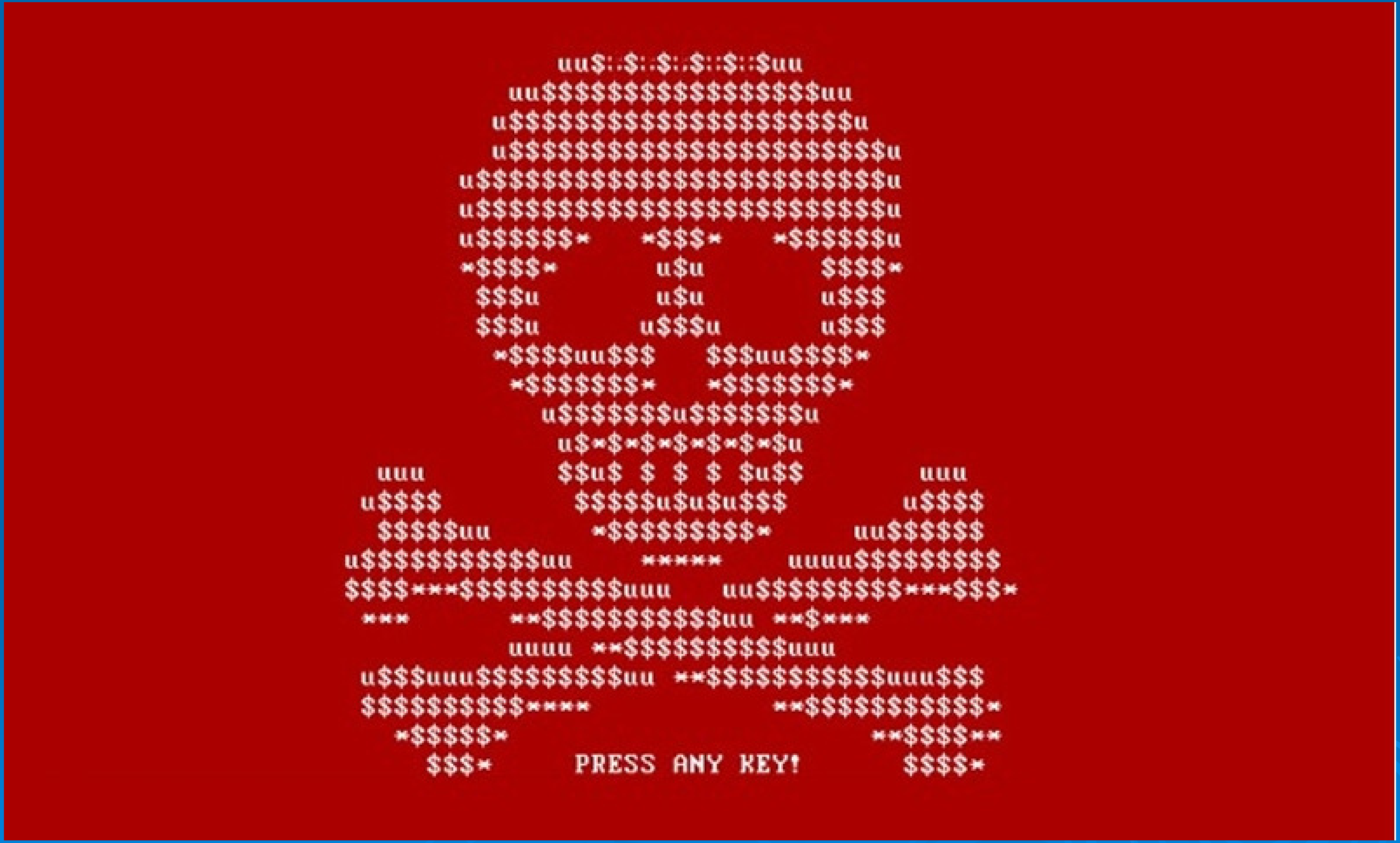
Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Security in the News

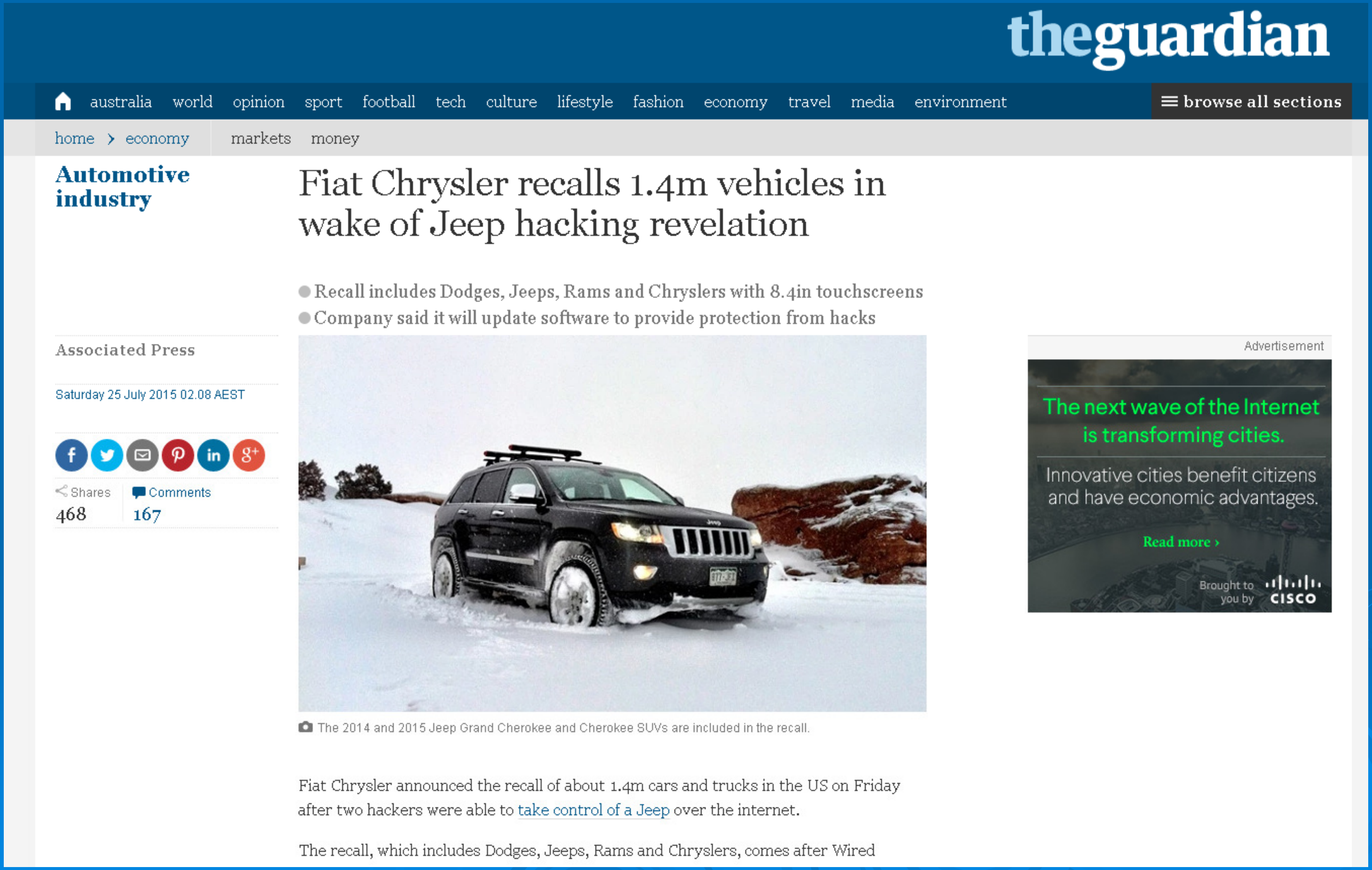


```
          uu$::$::$::$::$::$uu
       uu$$$$$$$$$$$$$$$$$uu
      u$$$$$$$$$$$$$$$$$$$$$u
     u$$$$$$$$$$$$$$$$$$$$$$$u
    u$$$$$$$$$$$$$$$$$$$$$$$$$u
    u$$$$$$$$$$$$$$$$$$$$$$$$$u
    u$$$$$$*   *$$$*   *$$$$$$u
    *$$$$*      u$u       $$$$*
     $$$u       u$u       u$$$
     $$$u      u$$$u      u$$$
      *$$$$uu$$$   $$$uu$$$$*
       *$$$$$$$*   *$$$$$$$*
         u$$$$$$$u$$$$$$$u
          u$*$*$*$*$*$*$u
uuu       $$u$ $ $ $ $u$$       uuu
u$$$$        $$$$$u$u$u$$$       u$$$$
 $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
           uuuu **$$$$$$$$$$uuu
  u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
  $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

Security in the News

- https://www.youtube.com/watch?v=MK0SrxBC1xs

Security Flaws are Expensive


theguardian
australia world opinion sport football tech culture lifestyle fashion economy travel media environment
browse all sections
home › economy markets money

Automotive industry

Fiat Chrysler recalls 1.4m vehicles in wake of Jeep hacking revelation

- Recall includes Dodges, Jeeps, Rams and Chryslers with 8.4in touchscreens
- Company said it will update software to provide protection from hacks

Associated Press

Saturday 25 July 2015 02.08 AEST

Shares 468 Comments 167

The 2014 and 2015 Jeep Grand Cherokee and Cherokee SUVs are included in the recall.

Fiat Chrysler announced the recall of about 1.4m cars and trucks in the US on Friday after two hackers were able to take control of a Jeep over the internet.

The recall, which includes Dodges, Jeeps, Rams and Chryslers, comes after Wired

- http://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking

Car Hacking is Not New

- Paper from 2010
  - Koscher, Karl, et al. Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy2010. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5504804

- Similar attacks on cars
  - https://www.youtube.com/watch?v=3jstaBeXgAs
  - https://www.youtube.com/watch?v=oqe6S6m73Zw
    - Earlier version of 'Jeep attack' by the same people

- A summary of attacks on different devices
  - TED talk: "All Your Devices Can Be Hacked"
    - http://www.youtube.com/watch?v=metkEeZvHTg

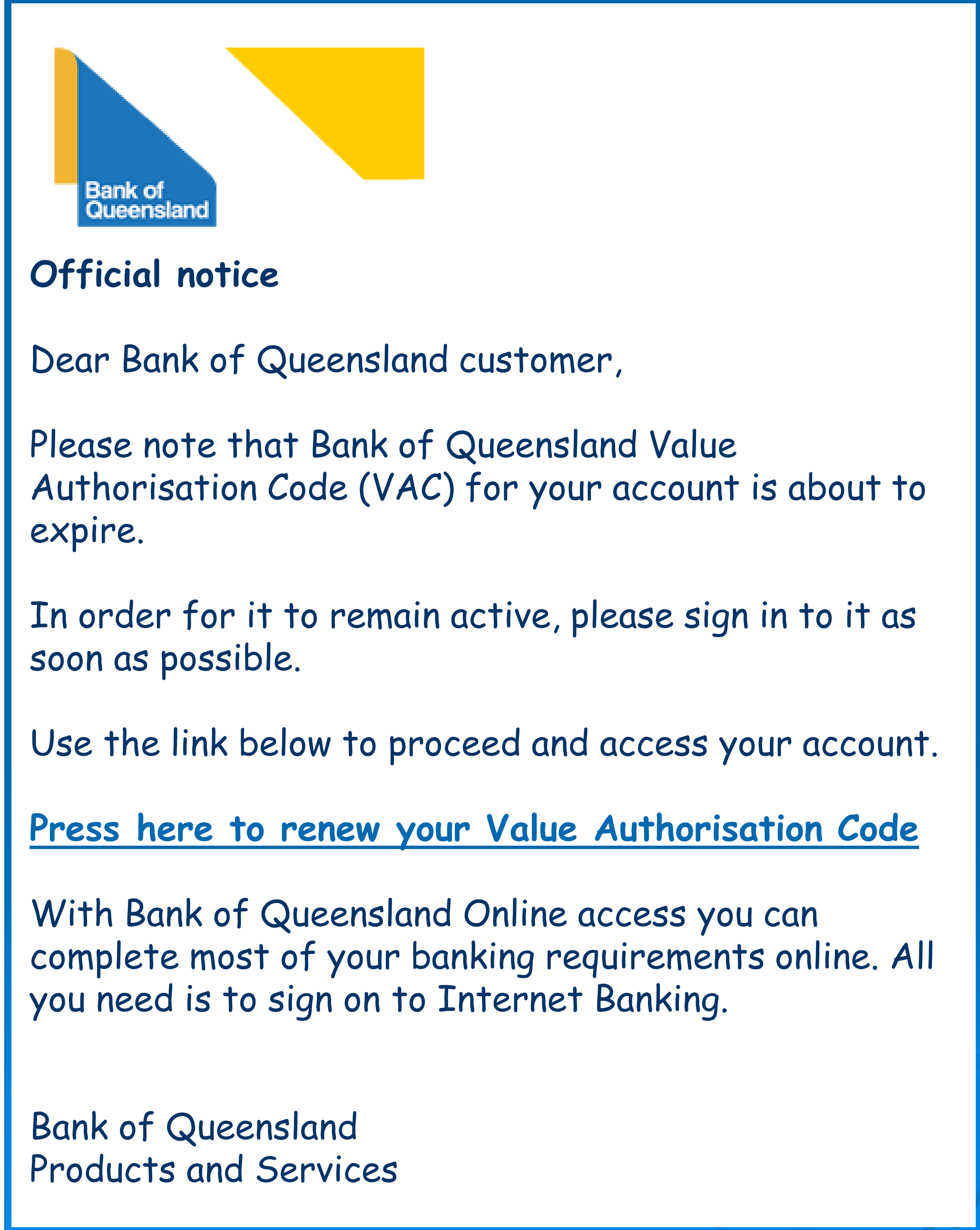
Internet of Things (IoT)

- Information Security is not just about securing servers, desktops, and smartphones, but also *things* like appliances, light bulbs, pacemakers, cars etc.

- "Cisco estimated that 50 billion devices and objects will be connected to the Internet by 2020."
  - Source: http://www.cisco.com/web/solutions/trends/iot/portfolio.html (defunct)

- Revised figures are now ~20 billion devices!

A Different Example



Official notice

Dear Bank of Queensland customer,

Please note that Bank of Queensland Value Authorisation Code (VAC) for your account is about to expire.

In order for it to remain active, please sign in to it as soon as possible.

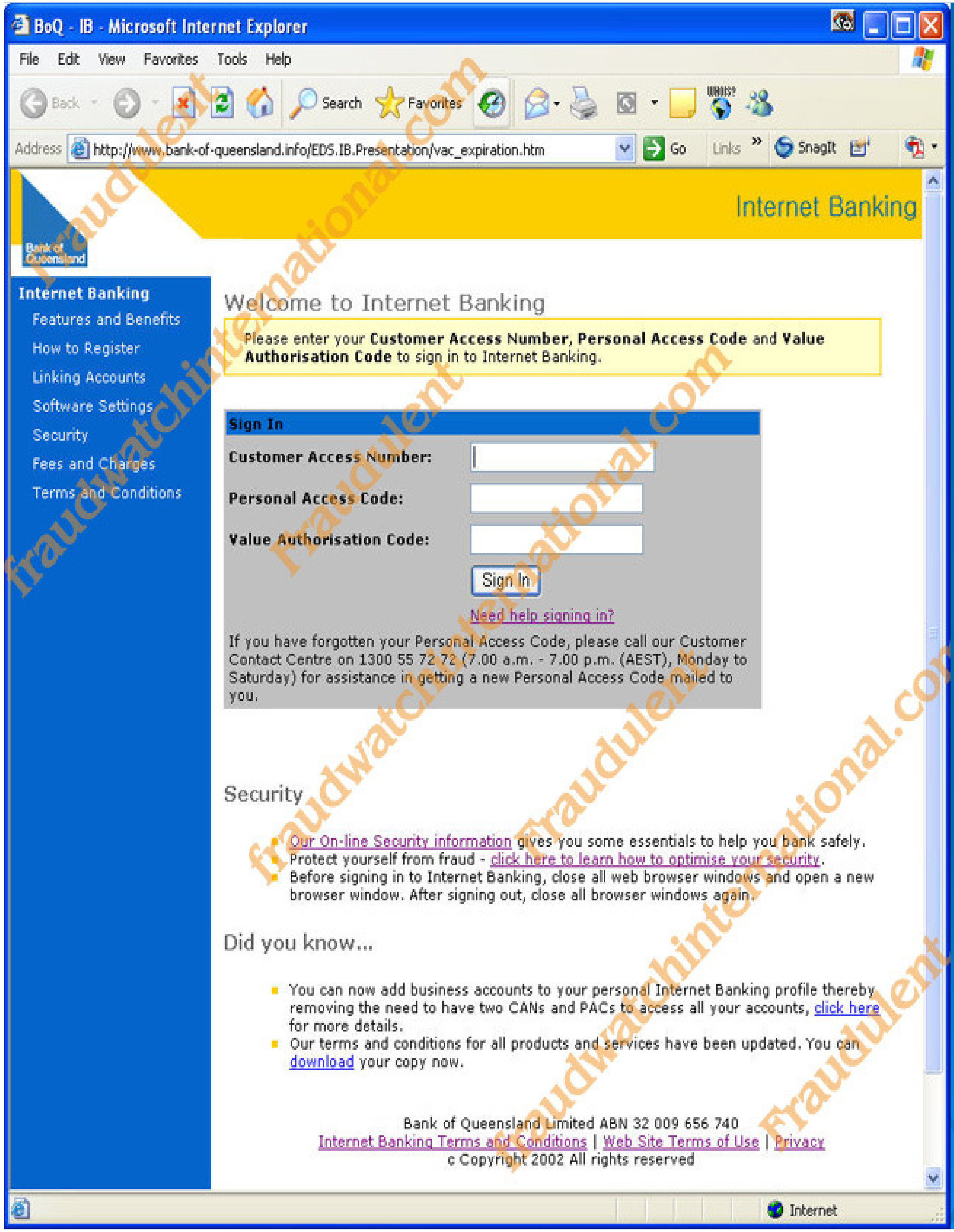
Use the link below to proceed and access your account.

Press here to renew your Value Authorisation Code

With Bank of Queensland Online access you can complete most of your banking requirements online. All you need is to sign on to Internet Banking.

Bank of Queensland
Products and Services

- Please read this email
- What’s the security problem?
- Key words that come to mind?
  - Identity Theft
  - Phishing
    - attempt to obtain sensitive information such as usernames, passwords etc. by masquerading as a trustworthy entity in electronic communication.
  - Social Engineering
  - Trust
  - Authenticity


BoQ - IB - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links SnagIt
Bank of Queensland
Internet

Address: http://www.bank-of-queensland.info/EDS.IB.Presentation/vac_expiration.htm

Internet Banking

Internet Banking
- Features and Benefits
- How to Register
- Linking Accounts
- Software Settings
- Security
- Fees and Charges
- Terms and Conditions

Welcome to Internet Banking

Please enter your **Customer Access Number, Personal Access Code** and **Value Authorisation Code** to sign in to Internet Banking.

Sign In

Customer Access Number:

Personal Access Code:

Value Authorisation Code:

Sign In

Need help signing in?

If you have forgotten your Personal Access Code, please call our Customer Contact Centre on 1300 55 72 72 (7.00 a.m. - 7.00 p.m. (AEST), Monday to Saturday) for assistance in getting a new Personal Access Code mailed to you.

Security

- Our On-line Security information gives you some essentials to help you bank safely.
- Protect yourself from fraud - click here to learn how to optimise your security.
- Before signing in to Internet Banking, close all web browser windows and open a new browser window. After signing out, close all browser windows again.

Did you know...

- You can now add business accounts to your personal Internet Banking profile thereby removing the need to have two CANs and PACs to access all your accounts, click here for more details.
- Our terms and conditions for all products and services have been updated. You can download your copy now.

Bank of Queensland Limited ABN 32 009 656 740
Internet Banking Terms and Conditions | Web Site Terms of Use | Privacy
c Copyright 2002 All rights reserved

- Users are tricked into revealing personal/private information
- Key words:
  - Identity Theft
  - “Phishing”
  - Social Engineering
- Basic problem here:
  - Lack of authentication
  - Is the sender really who he/she claims to be?
  - Trust
- What can you do to verify authenticity?
  - Check URL
    - Not 100%
    - DNS poisoning
    - ‘pharming’
      - cyber attack trying to redirect a website's traffic to another, malicious/fake site.
  - Check digital certificate
    - If HTTPS is used
- **More on these topics later…**

Important Source of Information

- **Blackboard Course Website**
  - Lecture Notes (available after the Lectures)
  - Assignments
  - Tutorials (questions & answers)
  - Handouts
  - Discussion Board

- **Course Profile**
  - Information about assessment etc.

Why are Lecture Notes not available *before* the Lecture?

- Lecture Notes often contain answers to class exercises and questions asked during class.
  - No fun if everybody has answers.

- Highly Dynamic – I often make last minute changes and corrections to slides.
  - Publishing the notes after the lecture guarantees you have the latest version.

Teaching and Learning Activities

- Lectures:
  - Friday 2:00pm – 3:50pm 50-T105

- Tutorials (Start in Week 2)
  - T01 Thursday 09:00 AM - 09:50 AM 67-142
  - T02 Thursday 10:00 AM - 10:50 AM 43-104
  - T03 Thursday 11:00 AM - 11:50 AM 67-142
  - T04 Thursday 14:00 AM - 14:50 AM 01-E303

- Please check on SInet, to be sure.
  - There may be changes

- Complete Tutorial Questions and Answers will be available on Blackboard

Teaching Plan

(indicative only – this is likely to change a bit)

Week Number	Lecture Topic	Notes
1	Admin, Introduction, Risk Management	
2	Access Control, Authentication	Tutorial 1
3	Authentication Protocols, Biometrics	Tutorial 2; Assignment out
4	Authorisation, Access Control	Tutorial 3
5	Security Models, Information Theory	Tutorial 4
6	Information Theory, Cryptography	Tutorial 5
7	Symmetric Cryptography	Tutorial 6

Teaching Plan (2)

Week Number	Lecture Topic	Assessment
8	Asymmetric Cryptography	Tutorial 7
9	No lecture – Assignment DUE 4:00 PM	Assignment due (Friday); Tutorial 8
	Mid Semester Break	
10	Network Security	Tutorial 9
11	Payment Card Industry (PCI) Security	Tutorial 10
12	Cloud Computing Security	Tutorial 11
13	Industrial Control System (ICS) Security; Revision; Info on Final Exam	Tutorial 12 – revision

Assessment

- In-Class Quiz (20%)
  - 20 multiple choice (20%)
  - CLOSED Book
- Assignment (20%)
  - Written Report
  - More details later..
- Final Exam (60%)
  - During examination period at end of semester
  - Open book
- See also Course Profile for details

Determination of Final Grade COMS3000

Final Grade	Overall Percentage
7 (High Distinction)	85 - 100%
6 (Distinction)	75 - 84%
5 (Credit)	65 - 74%
4 (Pass)	50 - 64%
3 (Fail, limited pass)	45 - 49%
2 (Fail)	20 - 44%
1 (Fail)	0 - 19%
X	No work submitted or tests/exams attempted.

- Marks: Weighted arithmetic mean of assessment items
- Additional condition:
  - To pass this course, you need to achieve **at least 40%** in the final exam.

Determination of Final Grade COMS7003

Final Grade	Overall Percentage
7 (High Distinction)	88 - 100%
6 (Distinction)	78 - 87%
5 (Credit)	68 - 77%
4 (Pass)	53 - 67%
3 (Fail, limited pass)	48 - 52%
2 (Fail)	23 - 47%
1 (Fail)	0 - 22%
X	No work submitted or tests/exams attempted.

- Same as COMS3000, but with 3% higher grade cut-offs.
- Additional rule:
  - To pass this course, you need to achieve at least 45% in the final exam.

Assignments

- Individual work
- Research and write a report on a topic of Information Security
- Focus
  - Critical thinking and discussion
  - Not just summary of a few papers, or worse, just wikipedia
  - Use high quality sources (peer reviewed papers)

- Different versions for COMS3000 and COMS7003

- Assignment:
  - Out: Week 3
  - Due: Week 9 (Friday 4PM)

- Submit hardcopy (via Faculty assignment chute) AND electronic version (Blackboard).
- The assignment is considered as submitted only when BOTH the hard copy AND the electronic version have been submitted.

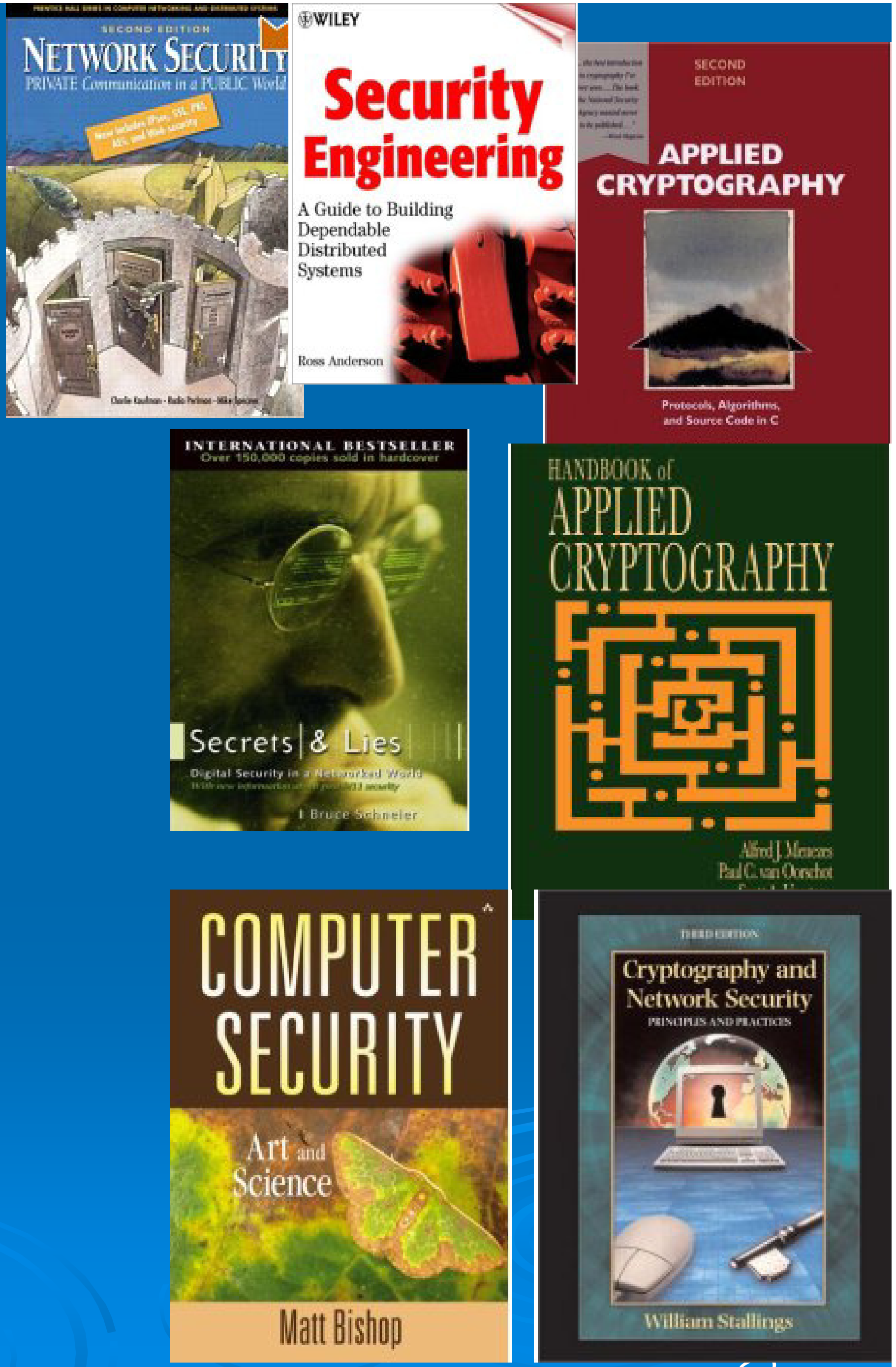
Learning Material

- Textbook
  - You are **not required to buy a textbook** for this course

- All required learning material will be provided on the course web site:
  - Lecture slides
  - Tutorials: Questions and Answers
  - Additional Reading Material, Handouts
  - Assignments

Recommended Books

- **For more background**
  - **You are not required to buy any of these**
  - **Should also be available at the Library**
- **Charlie Kaufman et al., Network Security: Private Communication in a Public World, Prentice Hall**
  - **Highly recommended**
  - **Covers a significant portion of COMS3000/7003 content**
- **Ross Anderson, Security Engineering, Wiley**
  - **Excellent book on practical aspects of Security**
- **Bruce Schneier, Applied Cryptography, Wiley**
  - **Covers most relevant cryptographic algorithms**
- **Bruce Schneier, Secret and Lies, Wiley**
  - **Easy to read, not very technical, high level overview**
- **Albert Menezes et al., The Handbook of applied Cryptography**
  - **Focus on the maths of cryptography**
  - **free online version: www.cacr.math.uwaterloo.ca/hac/**
- **William Stallings, Cryptography and Network Security, Addison Wesley**
  - **Focus on Network Security and protocols**
- **Matt Bishop, Computer Security, Prentice Hall**
  - **Focus on System Security**


SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World
Charlie Kaufman · Radia Perlman · Mike Speciner
WILEY
Security Engineering
A Guide to Building Dependable Distributed Systems
Ross Anderson
SECOND EDITION
APPLIED CRYPTOGRAPHY
Protocols, Algorithms, and Source Code in C
INTERNATIONAL BESTSELLER
Over 150,000 copies sold in hardcover
Secrets & Lies
Digital Security in a Networked World
Bruce Schneier
HANDBOOK of APPLIED CRYPTOGRAPHY
Alfred J. Menezes
Paul C. van Oorschot
COMPUTER SECURITY
Art and Science
Matt Bishop
THIRD EDITION
Cryptography and Network Security
PRINCIPLES AND PRACTICES
William Stallings

Teaching Style

- I would like the Lectures to be interactive
- Why?
  - It’s more interesting for you and me
  - You will learn more
- Please ask any questions anytime
- I will be asking questions
- There will be class exercises, discussion of issues in small groups
  - Your active participation is required

Feedback Appreciated

- If you have comments about:
  - Lectures
  - Assignments
  - Website
  - Teaching style
  - …
- Please make them!
  - The earlier the better
- Via the discussion board, via email, in person,…

Any questions so far?

Security

- What is Security?
- Webster Online Dictionary:
  - Security: "*the quality or state of being secure*"
  - Secure: "*free from risk of loss*"
- Security is about dealing with the potential loss of or damage to **assets**
- From a Business Perspective, potential damage to assets is treated as a ***Risk***
- General *Risk Management* methods can be applied

How to Deal with Risk

- As a business, how can you deal with Risks
  - (We will define Risk more formally later)
  - For example: Burglary or fire in a bank

- Three things you can do with a Risk:
  - Accept it
    - e.g. We accept the risk of a meteorite impact
  - Transfer it
    - → Insurance (Fire, burglary, etc.)
  - Reduce (mitigate or 'treat') it
    - reduce likelihood and/or impact
    - How can we do this here?
      - Alarm system, Guards etc.
      - Install a sprinkler system

- This course is mainly about the third option
  - Reducing the risk of 'damage' to **information assets** by means of ***Protective Measures***

Types of Protective Measures

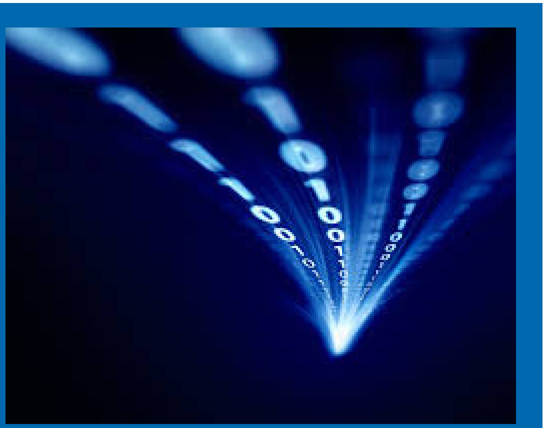
- Preventative Measures
  - Prevent assets from being ‘damaged’
- Detective Measures
  - Allow detection ***when*** an assets has been ‘damaged’, ***how*** it has been damaged and ***who*** caused it
- Reactive Measures
  - Allow recovery from ‘damage’ to assets

Protective Measures

Example from the Physical World

- You want to protect valuable items inside your home from burglary.
- Preventative Measures, Examples?
  - Door locks, window bars, a moat(?)
- Detective Measures, Examples?
  - Burglar Alarm, Security cameras
- Reactive Measures, Examples?
  - Call the police

Information Security



- Security is about dealing with potential ‘damage’ to assets
- What is Information Security?
  - Deals with potential ‘damage’ to information assets
- The aim is to protect information assets from ‘damage’
- How can information assets be ‘damaged’ or compromised?
  - Can you think of an example?

Information Security

- Information Assets can be compromised or ‘damaged’ in terms of:

- Confidentiality, Privacy, Secrecy
  - Prevention of unauthorised disclosure of information
  - Example:
    - Company secrets leaking to competitors, e.g. Coca Cola recipe

- Integrity
  - Prevention of unauthorised modification of information
  - Example:
    - Student hacks UQ server and changes his/her grades

- Availability
  - Prevention of unauthorised withholding of information or services
  - Examples:
    - A hacker hacks a file server and crashes it. Access to data is denied
    - Denial of Service (DoS) attacks

Aspects of Information Security

- Definitions of aspects of Information Security vary
- Most commonly, it is defined as the following 5 aspects:

- **C**onfidentiality, Privacy, Secrecy
- **I**ntegrity
- **A**vailability

"*CIA Triad*"

- **Authenticity**
  - Making sure the author/sender of a message is as it is claimed
  - Example for an attack on Authenticity?
    - Email with forged sender address (Phishing Example)
- **Non-repudiation**
  - Non-repudiation ensures that the maker of a statement, or signer of a contract, will not be able to successfully challenge the validity of the statement or contract.
    - e.g. "I never authorised that purchase", "I never agreed to that"
  - How can non-repudiation be implemented, in general and in the context of Information Security?
    - signatures, digital signatures

Risk Management

- What is RISK MANAGEMENT?
  - (in the context of information security)

"The process concerned with identification, measurement, control and minimisation of security risks in information systems to a level commensurate with the value of the assets protected."

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Risk Management

- Risk management helps information systems (IS) management strike an (informed) economic balance between the impact of risks and the cost of protective measures.

- Risk management is the total process of identifying, measuring, controlling, and minimizing or eliminating the likelihood and/or impact of an attack.

- It includes risk assessment; cost benefit analysis; selection, implementation, and evaluation of security features and countermeasures; and an overall security review.

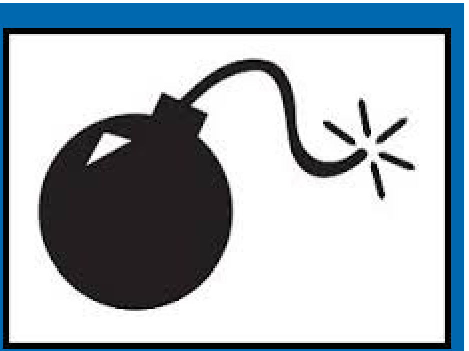
Risk – A Definition

- RISK
  - "The likelihood that a particular threat using a specific attack, will exploit a particular vulnerability of a system that results in an undesirable consequence."

- There exist a number of different definitions of Risk with slightly different meanings.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Threat - Definition



- “Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or the denial of service.”
  - Examples:
    - Hacker attack, Fire, etc.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Vulnerability - Definition

- “Weakness in an information system, cryptographic system, or other components (e.g... , system security procedures, hardware design, internal controls) that could be exploited by a threat.”
  - Examples:
    - Un-patched web server
    - Lack of firewall
    - Unlocked door
      - Example of *physical security*, which is an important part of Information Security

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Risk Assessment (Risk Analysis/Evaluation)

"A process of analyzing THREATS to, and VULNERABILITIES of, an information system and the POTENTIAL IMPACT the loss of information or capabilities of a system would have. The resulting analysis is used as a basis for identifying appropriate and cost-effective counter-measures."

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

Risk Management

- Three things to do with a Risk (recap)
  - Accept it
    - What’s the acceptable level of Risk?
  - Transfer it → Insurance
  - Reduce it → Risk Mitigation
    - Apply *‘security controls’*
      - safeguards or countermeasures to reduce risk
    - Examples in the context of Information Security:
      - Install a firewall, IDS, IPS, …
      - User Training
      - Guard dogs
      - Create a Security Policy

- “Residual Risk”:
  - The proportion of Risk that remains after security measures have been applied

Risk Management

- IT Manager have limited resources to spend on security
- Risk Management helps to determine how these resource can be used most efficiently
- It can help answer questions like these:
  - “Should we spend $100’000 to upgrade the company’s firewalls?”
  - “Should we buy a an insurance policy against data loss due to a fire?”

Quantitative Risk Analysis

- We would like some quantitative description of Risk
  - (or Risk Magnitude)
- Any ideas?
- RISK = Expected Cost of Damage = Impact * Likelihood

- Two main questions:
  - What's the probability of a loss event occurring?
    - Probability of a major flood in Brisbane in the next year ≈ 1%
    - Can be based on historical data
  - What's the impact (loss) in terms of $?
    - Unavailability of a company web site for one day might result in $100,000 of lost business
    - Leaking of secret Coca-Cola recipe → Millions of dollars

Quantitative Risk Analysis Parameters

- ARO (Annualised Rate of Occurrence)
  - Expected number of times a loss event occurs within a year
  - Example:
    - Damage to a data centre due to Meteorites can be estimated to occur every 100,000 years
    - ARO =?
    - ARO = 0.00001 = 10^{-5}

- SLE (Single Loss Expectancy)
  - The impact (loss) of a loss event occurring in $
  - Example:
    - Complete loss of data centre due to meteorite impact: $10 Million

- ALE (Annualised Loss Expectancy)
  - Expected (average) loss per year due to a Risk
  - ALE = ?
  - ALE = ARO * SLE (= 0.00001 * $ 10 Million = $100)
  - ALE can serve as a ‘measure’ of Risk exposure, for example to prioritise security measures.

Simple Example

- From a business perspective, should a company install a firewall system for $40,000/year that reduces the probability of the Web Server being hacked to ≈0?

- On average the company's web server is hacked once every 3 years
  - Annualised Rate of Occurrence, ARO = ?
  - ARO = 1/3
- In such a case, we expect the server to be down for 4 hours
- The Web server hosts an eCommerce application that generates $10,000/hour
- The cost of an external specialist security team to fix the problem is estimated to cost $4000.
- Customer dissatisfaction with the unavailability of the service and loss of reputation is quantified at $40'000.

- Single Loss Expectancy, SLE = ?
  - SLE = $84,000 = $40,000 + 4*$10,000 + $4,000

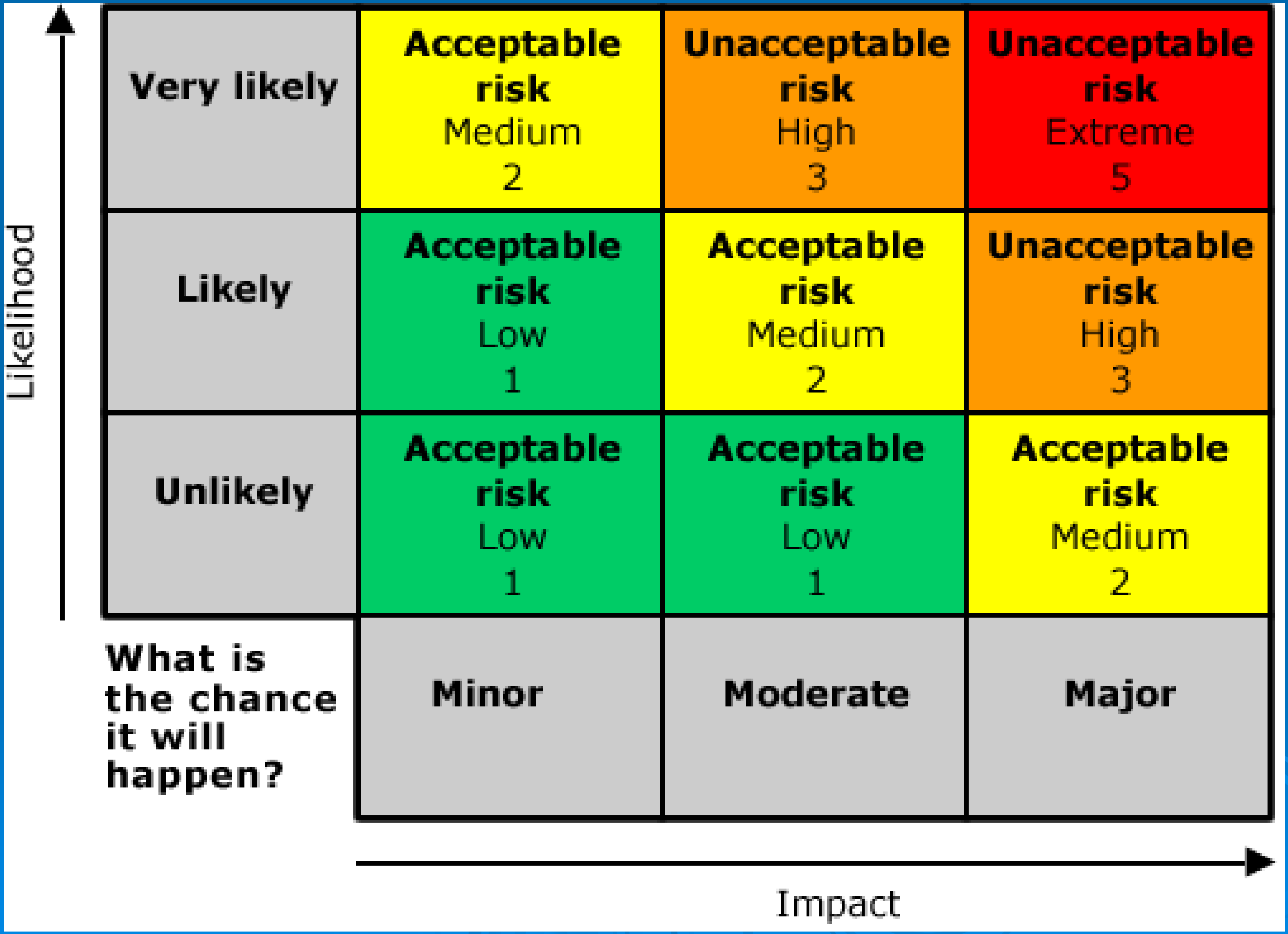
- Annualised Loss Expectancy, ALE=?
  - ALE= SLE * ARO = 1/3 * $84'000 = $28,000

- Conclusion?
  - → The company is better off accepting or bearing the risk.

Quantitative vs. Qualitative Risk Analysis

- In practice, it is often very difficult to
  - Assign probabilities to loss events
  - Quantify the cost/impact of loss events
- Often, qualitative methods are used
  - Examples:
    - Likelihood: high, medium, low
    - Impact Rating: very high, high, medium, low, very low
- If Risks cannot be quantified, they are often ranked: highest to lowest

Risk Assessment Matrix



Very likely	**Acceptable risk** Medium 2	**Unacceptable risk** High 3	**Unacceptable risk** Extreme 5
Likely	**Acceptable risk** Low 1	**Acceptable risk** Medium 2	**Unacceptable risk** High 3
Unlikely	**Acceptable risk** Low 1	**Acceptable risk** Low 1	**Acceptable risk** Medium 2
What is the chance it will happen?	**Minor**	**Moderate**	**Major**

Likelihood

Impact

Example from Cryptogram

Bruce Schneier’s Monthly Security news email

www.counterpane.com/crypto-gram.html

“The other week I visited the corporate headquarters of a large financial institution on Wall Street; let's call them FinCorp. FinCorp had pretty elaborate building security. Everyone -- employees and visitors -- had to have their bags X-rayed.

Seemed silly to me, but I played along. There was a single guard watching the X-ray machine's monitor, and a line of people putting their bags onto the machine. The people themselves weren't searched at all. Even worse, no guard was watching the people. So when I walked with everyone else in line and just didn't put my bag onto the machine, no one noticed.

It was all good fun, and I very much enjoyed describing this to FinCorp's VP of Corporate Security.

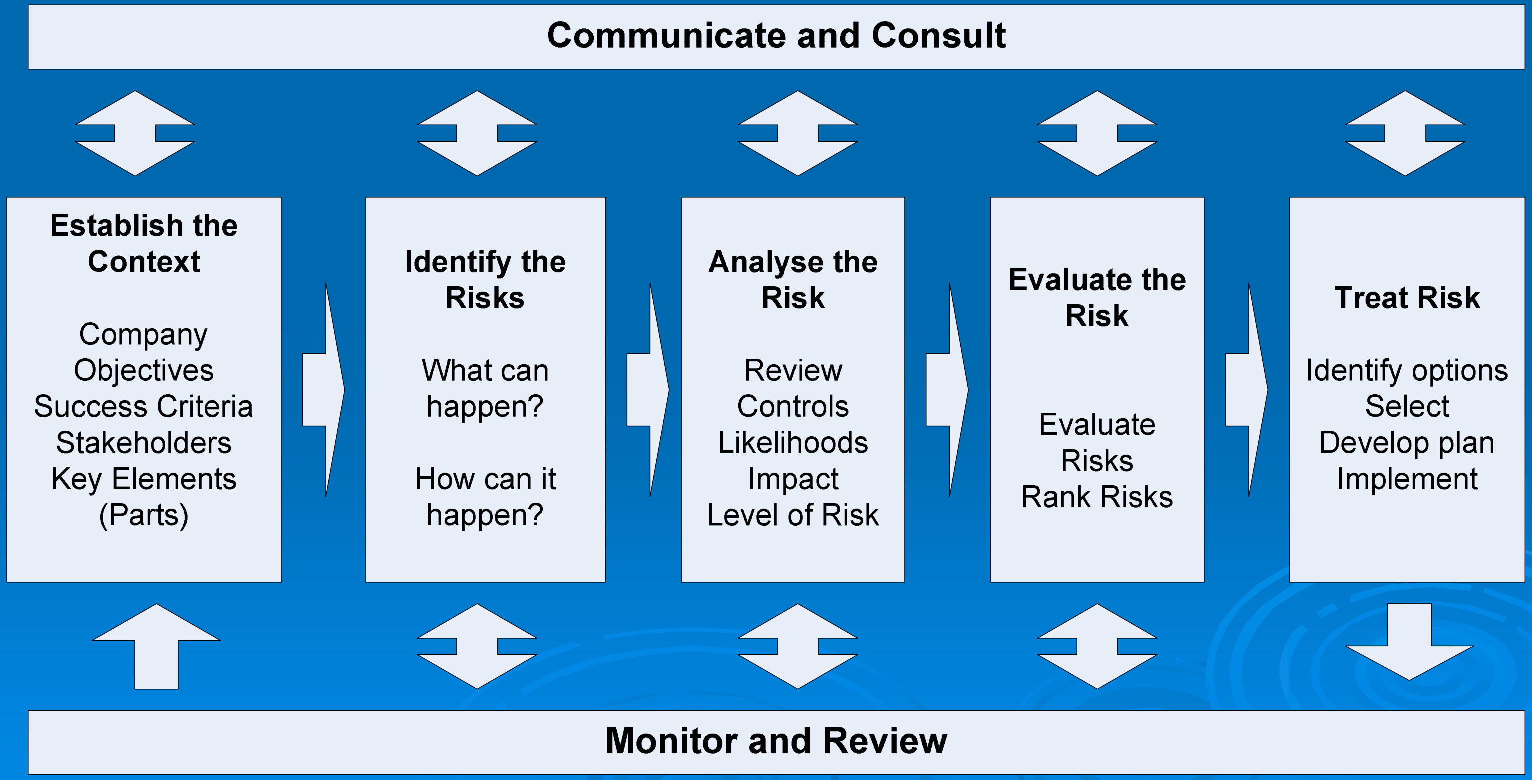
Example from Cryptogram (2)

FinCorp's VP of Corporate Security explained to me that he got a $5 million rate reduction from his insurance company by installing that X-ray machine and having some dogs sniff around the building a couple of times a week.

I thought the building's security was a waste of money. It was actually a source of corporate profit.”

Risk Management

- Relevant Australian and New Zealand Standard:
  - AS/NZS ISO 31000:2009
  - “Risk Management Principles and Guidelines”



Communicate and Consult

Establish the Context

Company Objectives
Success Criteria
Stakeholders
Key Elements (Parts)

Identify the Risks

What can happen?

How can it happen?

Analyse the Risk

Review Controls
Likelihoods
Impact
Level of Risk

Evaluate the Risk

Evaluate Risks
Rank Risks

Treat Risk

Identify options
Select
Develop plan
Implement

Monitor and Review

Any questions?