Managing Risk

Security

Otago Polytechnic
Dunedin, New Zealand

How secure can we be?

Last time we said that perfect security is not possible. Given that, we need a way to talks about how secure we are or can be.

Security trade offs

You don't get security for free. You always have to trade away something to get it.

- Money
- Time
- Convenience
- Capability

Often we give up some combination of all of these.

Are we getting a good deal?

- Once we recognise that security has a cost, the question isn't really, "How secure can we be?"
- Instead, the question is, "How much are we willing to trade away in return for some security?"
- The thing is, people are not very good at assessing their security trade-offs.

Risk

- In our daily lives we may be able to tolerate our less than ideal decision making.
- In a business setting we need to do better.
- The name for this thing we need to measure is *risk*.
- Risk has a standard unit of measure. It's dollars per year.

Quantitative risk analysis

- One way to assess risk is to perform *quantitative risk analysis*.
- Full risk analysis is the work of specialists, but we can perform some basic analysis on our own.

Elements of risk analysis

To analyse our risk, we consider

- Assets - We assign a dollar value to them.
- Threats to those assets and the probability that the threatened harm will occur.
- Countermeasures that guard against the threatened harm or that reduce the amount of harm. These have a cost that we measure in dollars.

Am example

Suppose our business has a warehouse/shipping facility that ships orders to our customers at a rate of $1000 of revenue per hour.

- Asset: There is a computer system that the staff use to process orders.
- Threat: A power cut would take the system down.
- Countermeasure: We could get a UPS and backup generator.

Doing the numbers

- The value of the asset is $1000 per hour.
- Suppose we can expect 2 hours of power cuts in a typical year.
- Our risk (cost per hour of downtime) * (expected downtime per year) or $1000 * 2 = $2000
- This is called our *annual loss expectancy*, or ALE.

Doing the numbers

- Now suppose we can install and operate a backup power system for $6000.
- The system is expected to last for 5 years.
- Our annual cost is $6000/5 = $1200
- We call this the *annual cost of control*, or ACC

Doing the numbers

- Now we can look at the cost/benefit.
- (ALE without backup) - (ALE with backup) - (Cost of backup)
- $2000 - 0 - $1200 = $800
- In other words, backup power reduces a $2000 risk to an $800 risk. It's a good trade off.

Another example

Suppose that your boss comes in on Monday morning after having heard about cryptolocker-like malware attacks, in which an attacker encrypts all your files and then demands a ransom, say $25,000 in return for the encryption key. Your boss is in a near panic and insists on strong protective measures.

Determine the risk

- Your research shows that the probability of this malware intrusion event is only 0.0001 per week.
- This means that your risk exposure, or ALE is (cost of intrusion event) * (probability per week) * (52 weeks)
- ALE = $25,000 * 0.0001 * 52 = $130
- In other words the risk is very low.

However...

Control measures for this risk include anti-malware software and backup/recovery systems. So, the $130 of risk exposure in this case can be added to a larger risk exposure suite when determining the budget for malware protection and backup.