

Measuring Risk

Security

Otago Polytechnic
Dunedin, New Zealand

HOW SECURE CAN WE BE?

More to the point, how secure can we *afford* to 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*.
- ▶ Once we know how much risk we are exposed to, we can make smart decisions about how to reduce it.

MEASURING RISK

Risk is a factor of two things:

- ▶ The probability that something bad will happen
- ▶ The amount of harm that will result from it happening

ASIDE: CIA TRIAD

It's useful to identify the kinds of harm that can result from a security incident. The *CIA triad* is a helpful mnemonic for this.

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability

TWO TYPES OF ANALYSIS

- ▶ Qualitative: We rank our risks relative to each other and decide which ones receive priority.
- ▶ Quantitative: We assign a particular value, typically measured in dollars, to each element of risk.

QUALITATIVE ANALYSIS

The goal of *qualitative risk analysis* is to prioritise risks into categories like high, medium, and low priority.

QUALITATIVE ANALYSIS

To do this we evaluate

- ▶ The amount of harm caused by a possible event (high, medium, low)
- ▶ The relative probability of an event (high, medium, low)

QUALITATIVE ANALYSIS

Probability → Harm ↓	Low	Medium	High
Low			
Medium			
High			

QUANTITATIVE RISK ANALYSIS

- ▶ Another way to assess risk is to perform *quantitative risk analysis*.
- ▶ This is more complicated than qualitative analysis, but it gives us a way to set a budget for security improvement.

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

DOING THE NUMBERS

- ▶ Now we can look at the cost/benefit.
- ▶ $((\text{ALE without backup}) - (\text{ALE with backup}))$
- (Annual 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.
- ▶ Therefore, the probability this will happen in a given year is $0.0001 * 52 = 0.0052$
- ▶ 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, even though the cost and hence harm from an event is high.

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.

CONCLUSIONS

Qualitative analysis is, at least initially, fairly easy and is probably a good place to start.

Sometimes, especially when it comes to setting budgets, quantitative analysis provides more precise information and insight.