Threat-Based Security Engineering

An Engineering Approach to Managing Risk

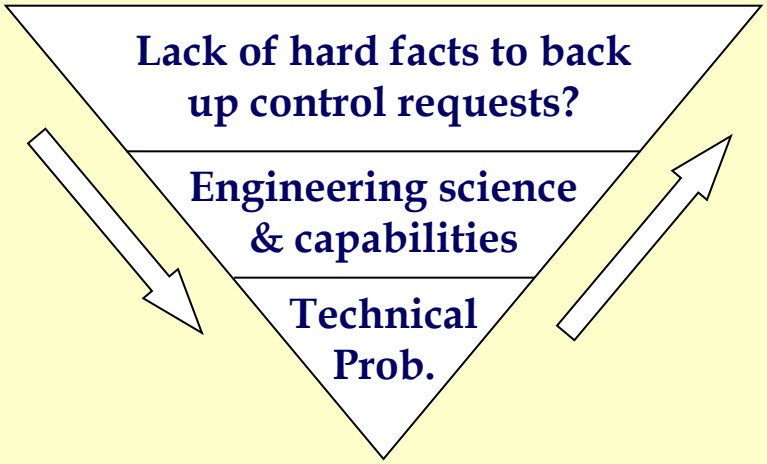
ISACA London Chapter Technical Briefing

23rd September 2004

John Leach

Overview

- Introduction
- The central issue
- A brief description of TBSE
- Some of the early TBSE results
- Where TBSE stands today – long-term and short-term benefits
- Where to from here – expectations for the years ahead

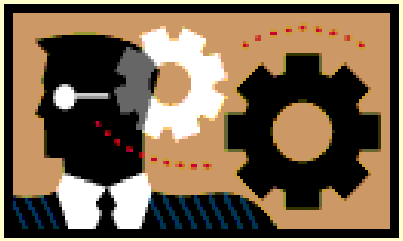


The Central Issue

- Life is an uphill struggle trying to convince others, sceptics often, to deploy needed controls and security measures when we don't have hard facts to back up control requirements.
- Requiring compliance with internal and external mandates is not enough. The desire is to add value to the business.
- This lack of hard facts is a source of immense frustration. How do we:
  - Set measurable protection targets for new systems?
  - Identify which are the measures which actually make a difference and contribute to addressing the security need?
  - Calibrate and set the levels for the controls we want to see?
  - Quantify how much security benefit we actually get from the controls we have deployed, without having to wait for something to break?
- Wouldn't it be grand if we could do these things? Not being able to do them makes managing the business extremely difficult and frustrating when the business is dependent on IT.

The Heart of the Problem

- We do not have a comprehensive understanding of what causes security outcomes, a theory describing the dynamics which lead to the security outcomes we see.
- What we need is a way to model these dynamics and do the sums to forecast the likelihood and characteristics of the outcomes we can expect to see.
- If we had this type of model, it would show us how to:
  - Measure the relevant inputs in the right form
  - Calculate the likelihood and characteristics of expected security outcomes
  - Forecast the effects varying each countermeasure would have on the expected outcomes



- Once we can do those, we will be in a position to:
  - Set objective measurable targets against which systems could be audited
  - Implement a metrics programme which provides meaningful answers
  - Forecast the residual risk of business disruption caused by the prevailing threats
  - Provide the board with clear and meaningful decision support.

We Need Risk Management to be an Engineering Science

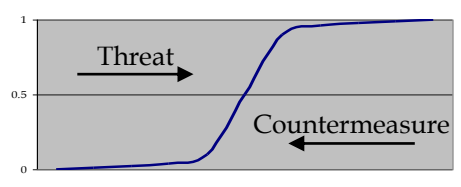
- Risk Management's not being a science doesn't mean that we have not been able to build effective security systems. Experience, skill and established practices have brought us a long way, though there has been a lot of guesswork involved.

The benefits of engineering are not always certain

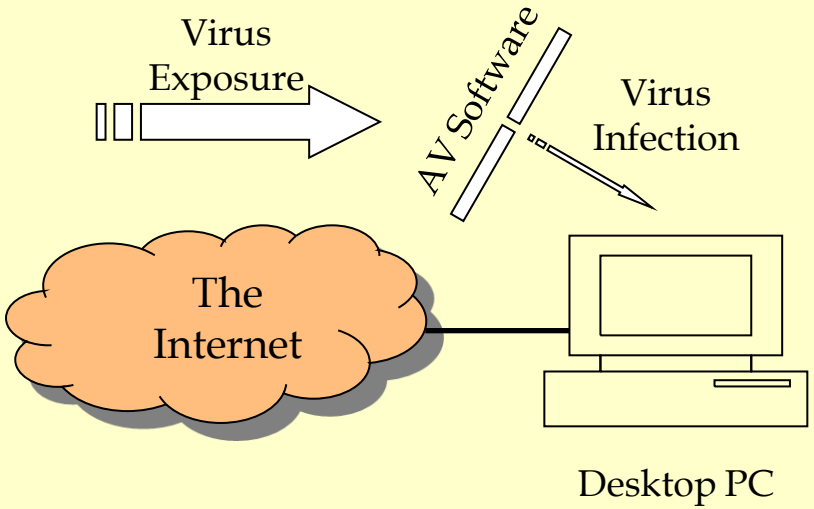
TBSE Solves that Underlying Central Technical Problem

- An analogy – the measures we take to keep ourselves free from diseases.
- Two complementary strategies:
  - We try to keep ourselves generally healthy;
  - We take specific measures in circumstances of heightened risk.
- Look at how the BoE's economists model and forecast inflation.
  - They need to forecast the effects of an economic stimulus (such as a 25 basis point interest rate cut) on an economic index (such as inflation). They don't do this by asking how each of millions of individual actors would respond to the stimulus and then aggregating over the whole economy.
  - In theory this approach might be valid but in practice it would be completely unworkable
  - Similarly, one shouldn't expect to forecast the effects of a security stimulus on a security index (such as risk) in that way.
- TBSE applies well-proven "econometrics-style" system-level, non-deterministic modelling techniques to the challenge of modelling Information Security risk

Examples of TBSE's Results

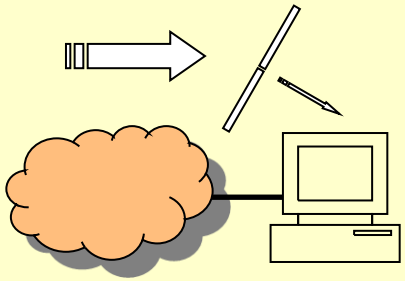


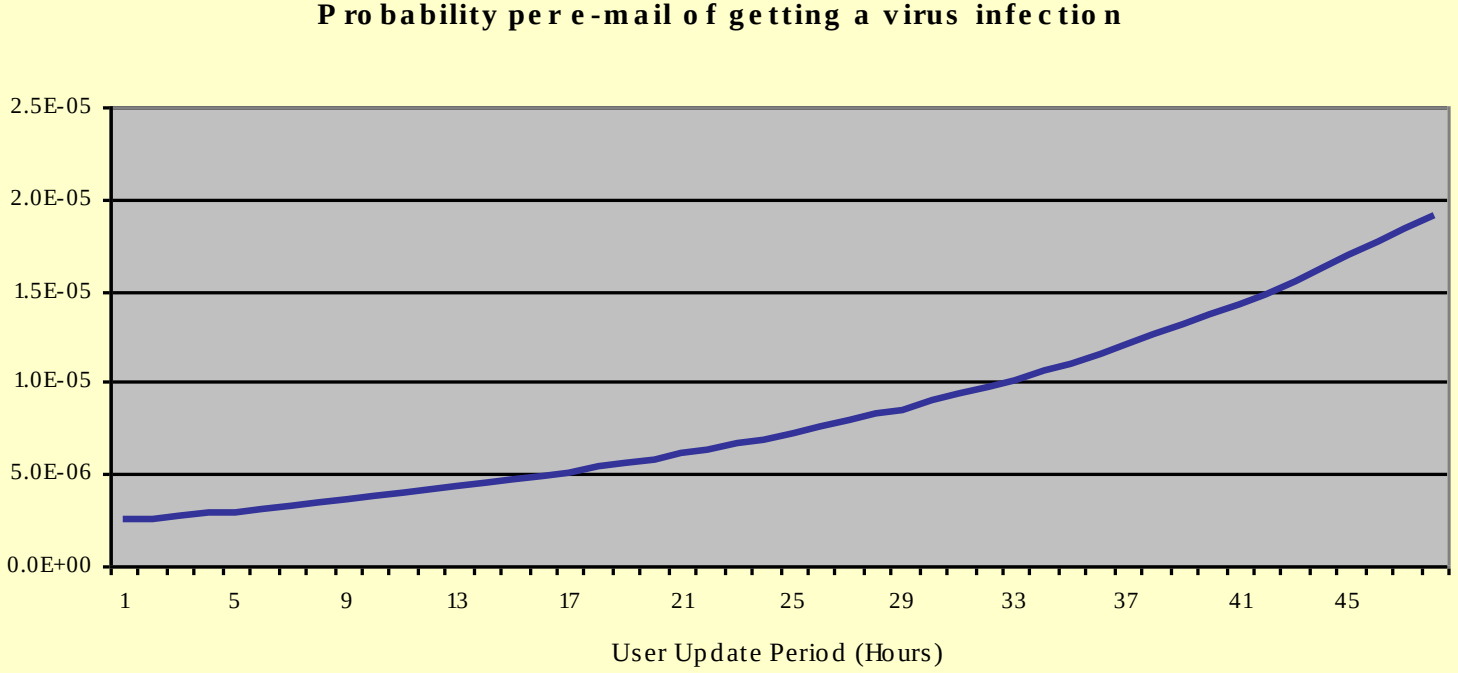
- To see what sort of result this type of modelling approach can generate, start by applying it to a simple and familiar problem:
  - An Internet-connected desktop PC protected against e-mail viruses by AV software.
  - The aim is to calculate the rate of infection from a given level of threat (exposure to e-mail viruses) as a function of how well the AV software is deployed



Examples of TBSE's Results

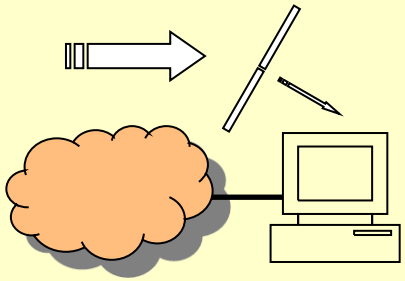
- TBSE shows how to measure the threat and how to describe the countermeasure analytically.
- The result is the probability, per e-mail, of the user getting a virus infection as a function of the time they take to apply new virus signature updates.

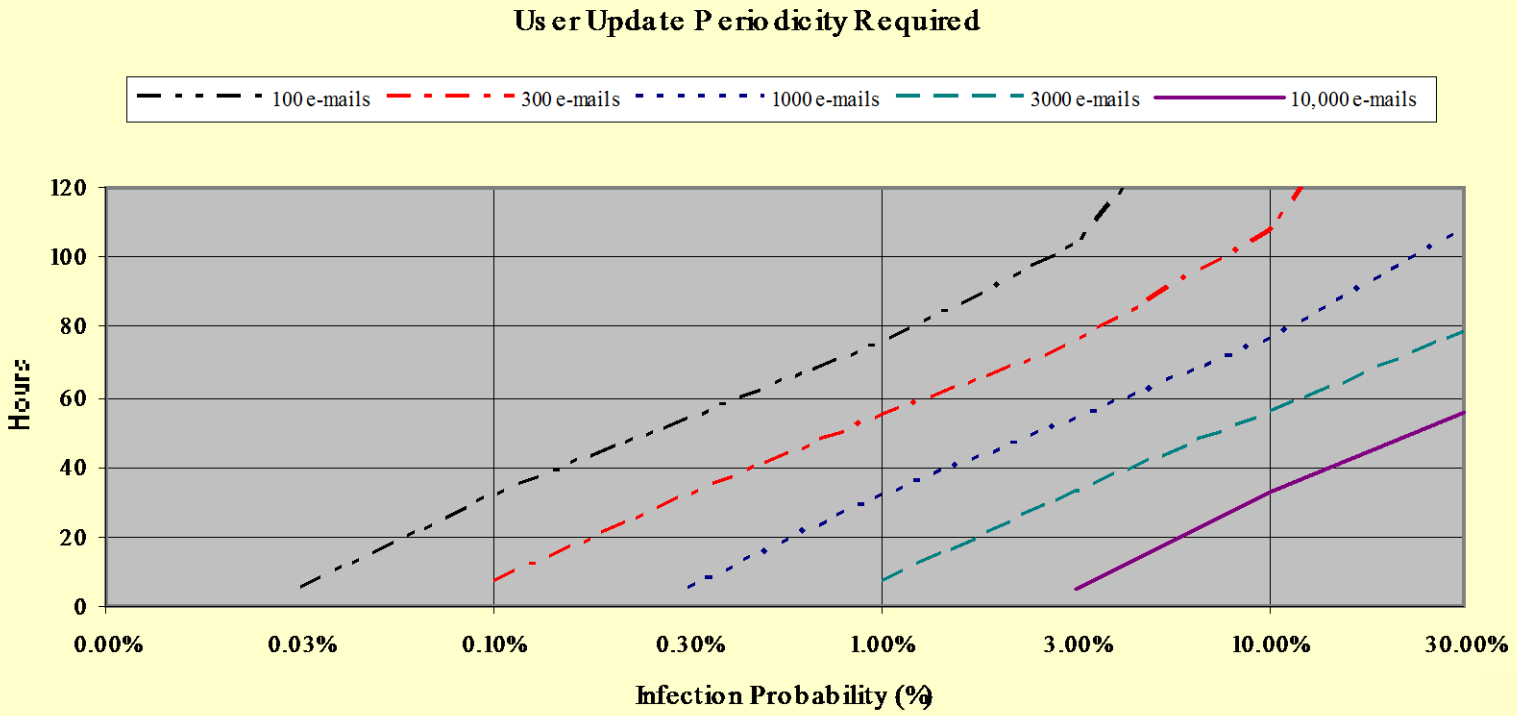




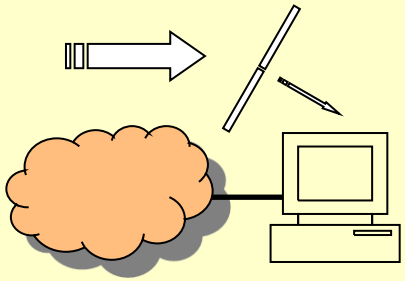
Examples of TBSE's Results

- A more useful form for the results is to show the probability of the user getting a virus infection as a function of the number of e-mails they receive.



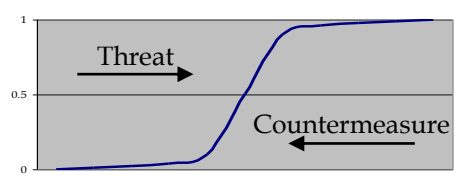


Examples of TBSE's Results

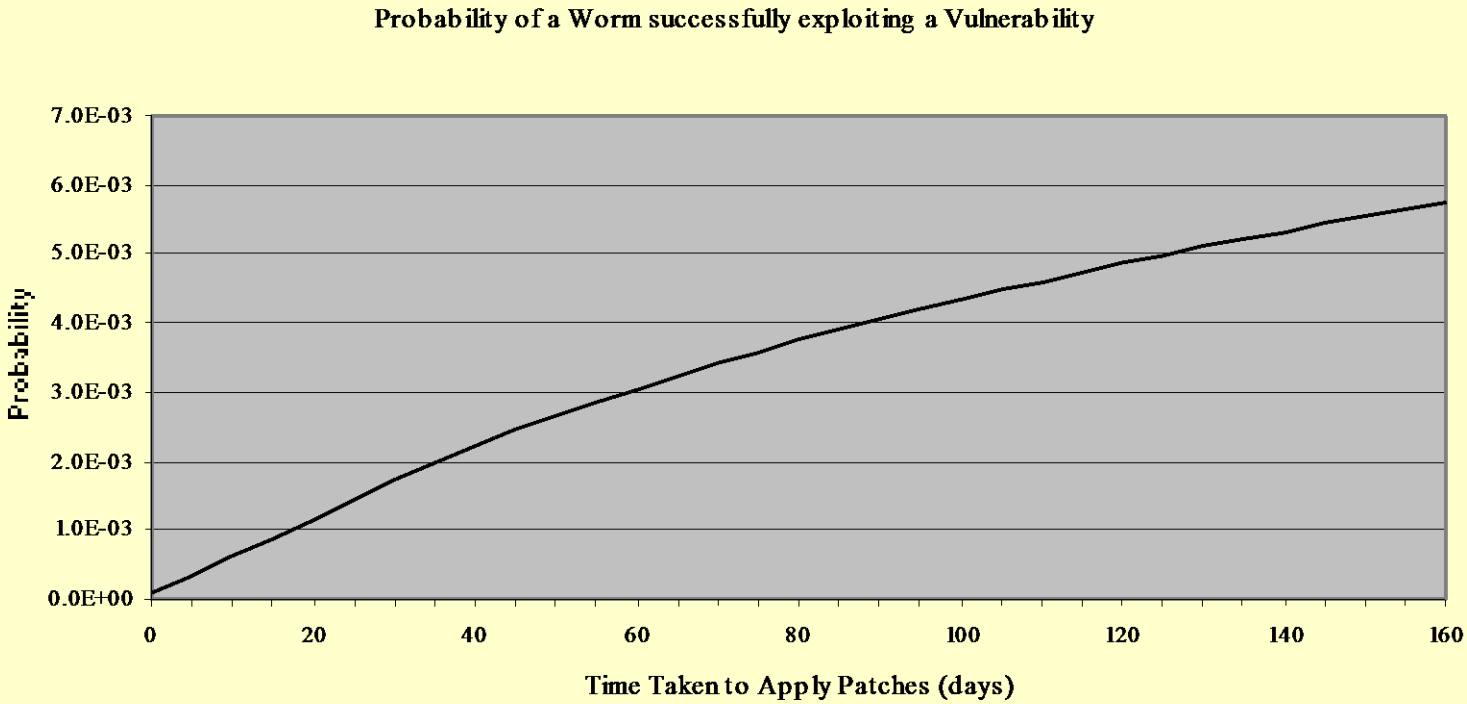


- The preceding results are based on out-of-date data
- The results from a recent collaboration with MessageLabs will appear shortly on the MessageLabs web site (www.messagelabs.com):
  - A chart showing the e-mail virus threat profile for today and for various past periods of high activity
  - The visitor inputs their AV and e-mail details
  - They get back a number, the risk they are running today in the form of the probability of an e-mail virus getting past their AV software defence.
  - The visitor can determine exactly how their risk would change if they were to change the frequency with which they check for new AV signatures
  - They can track how their risk rises or falls as the threat changes
  - They can work out what they need to do to maintain a constant level of protection against the ever-changing threat

Examples of TBSE's Results

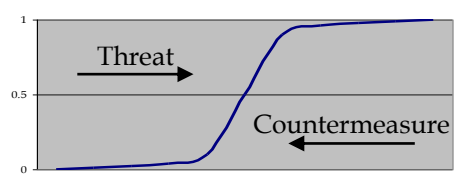


- The second simple and familiar problem is to look at the benefit of software patching to protect against worms.



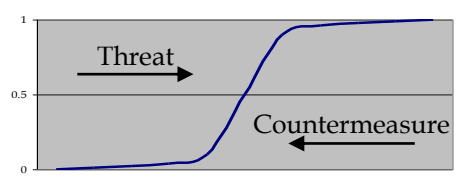
Information Security

Where TBSE Stands Today



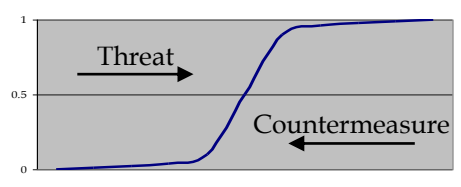
- The first objective has been to apply TBSE to well-defined, well-bounded problems:
  - The virus threat and the use of anti-virus software;
  - The worm threat and the use of software patching;
- These are two examples of generic threats countered by technical security solutions. TBSE can also be applied to threats countered by non-technical measures:
  - Unintentional staff security errors (c/m = education and awareness training);
  - Intentional abuse of privileges (c/m = security vetting, a strong security culture, increased deterrence).
- TBSE can be applied to more complex, increasingly comprehensive problems:
  - A single threat countered by several countermeasures
  - Two or three threats countered by a group of countermeasures
- It took years for economists to develop sophisticated econometrics models for complex systems such as national economies. It will be some time before we are able to develop comprehensive corporate security risk models.

Long-term and Short-term Capabilities

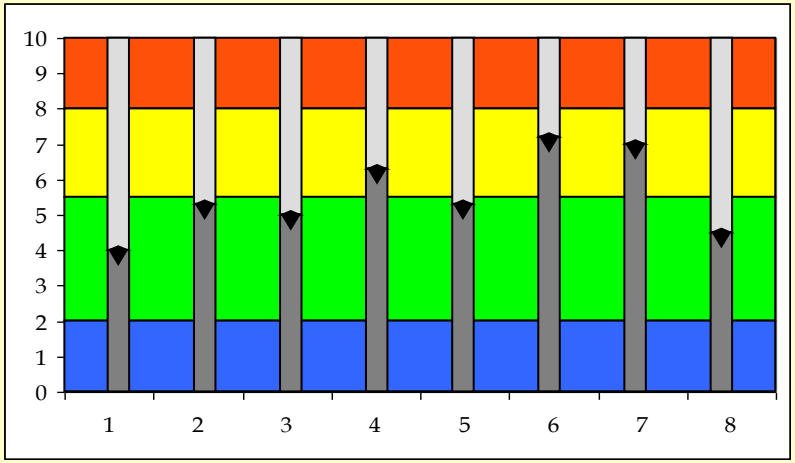


- TBSE makes Risk Management an engineering science
- Doing that would enable us to:
  - Set objective measurable protection targets for systems
  - Agree which controls are worthwhile and which provide little beyond simple compliance with policy
  - Set agreed control thresholds – agree what is inadequate, what is sufficient, what is over-heavy
  - Optimise security design to achieve targets in the most cost-efficient or operationally efficient manner
  - Measure key indicators (stresses, strengths and strains) to get a direct handle on exposure and risk
  - Provide quantified security benefit statements and perform RoI calculations
  - Forecast objectively the residual risk to the business of operations being disrupted by unplanned security events
  - Provide board-level management with the risk management decision support tools they want to see

Where can TBSE take Us?

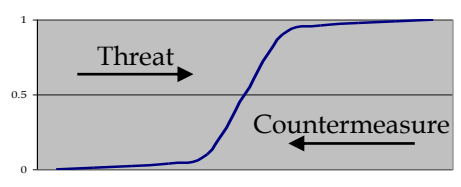


- Threat, countermeasure and risk barometers in the style of a Dashboard
  - Measure the top threats each month;
  - Measure how effectively each countermeasure is being applied;
  - Forecast the top risks over the next 3, 6, 12 months;
  - Adjust countermeasures accordingly to maintain risk within acceptable tolerances.



- Beyond that, we might anticipate:
  - New products such as Digital Risk insurance products;
  - New services measuring threat profiles and threat indices, calibrating security measures for corporate security assurance, new software products and management support tools.

Summary



- Within the Information Security field, we have wanted to model and quantify risk for many years, to make the subject more of a science and less of an art.
- Most past efforts have focussed on the deterministic part of the equation. I believe we have been starting from the wrong place. Deterministic approaches have failed to deliver the risk management capabilities we need.
- TBSE shows that we can apply non-deterministic techniques to modelling security risk and that we can then forecast security outcomes as a direct function of the measured threats and the security measures deployed.
- The impact of being able to model risk analytically will be felt across all areas of the field. This will bring new service and product opportunities, and new techniques to support management risk decision making.
- The prospects for the Information Security field are exciting, and we can look forward to the field at last being transformed into a modern engineering discipline.

Threat-Based Security Engineering

John Leach
☎ (+44) (0)1264 332 477
✆ (+44) (0)7734 311 567
✉ john.leach@jlis.co.uk