Threat-Based Security Engineering

How to Forecast Risk More Accurately than Michael Fish Forecasts the Weather

BCS-ISSG Annual Conference

26th March 2004

John Leach

Introduction – The State of Play Today

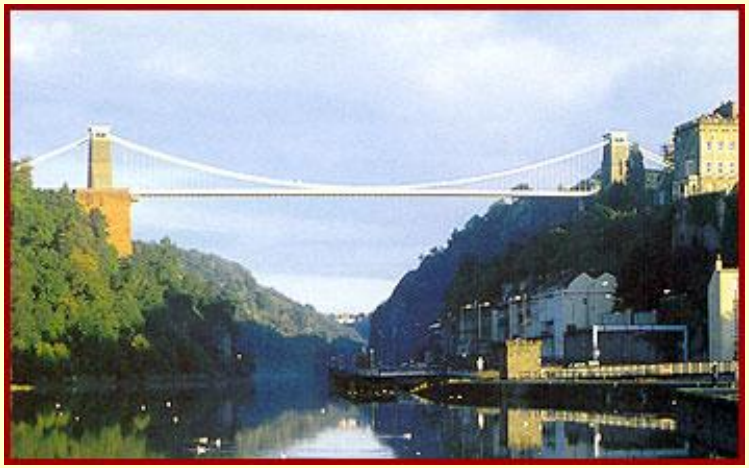
- We have been trying, for the past 20 years, to develop a reliable way to forecast Information Security risk and measure its benefits, without real success.
- This is a fundamental problem which remains unsolved with significant consequences. It is not just that we do not know how to show a security RoI, or how to quantify the benefits of security expenditures, or show that benefits are commensurate with costs. More fundamentally:
  - We don't have the terminology for describing security needs in measurable and objective terms;
  - Policy and practices are not rooted in any analysis of security outcomes.
- Crucially, the effect of this is that we cannot reliably quantify the likelihood of business operations or plans being disrupted by unplanned security events.
- This makes managing the business difficult and frustrating when the business is dependent on IT.
- While other areas of Information Management have moved forward, Information Security has remained a Dark Art.

The Fundamental Problem in need of a Solution

- At the core of these shortcomings is a single problem we have yet to solve.
- We need to develop a comprehensive understanding of how security threats combine with security weaknesses and interact with security countermeasures to result in the security outcomes we see.
- We need:
  - A model to describe these dynamics;
  - The tools, techniques, algorithms, etc. with which to measure relevant inputs in the right form and to calculate from those inputs the likelihood and characteristics of expected security outcomes.
- In the absence of such techniques, the risk management solutions we have today are blind. They are built around established practices though without those practices being rooted in an analysis of how countermeasures affect outcomes.
- Being blind doesn't make them ineffective. It does make them inefficient as we have no way of showing if they are accurate or reliable.

Risk Management Needs to be More Scientific

- Being blind doesn't make them ineffective. Experience, skill and established practices have brought us a long way.
- But we can't claim our security systems have been built accurately when there has been so much guesswork involved.



The Benefits of Engineering?

How To Move Forward?

- Past risk quantification efforts have tended to treat each individual security incident as being essentially deterministic, a well defined event caused by well defined, predictable and repeatable interactions.
- The belief underpinning this type of approach is that if we knew everything we needed to know, we would be able to predict precisely what the security outcome would be for any situation. Then: Probability (outcome) = Probability (situation arising).
- In principle, this approach might be right. In practice, it is simply not tractable.

The Deterministic Approach

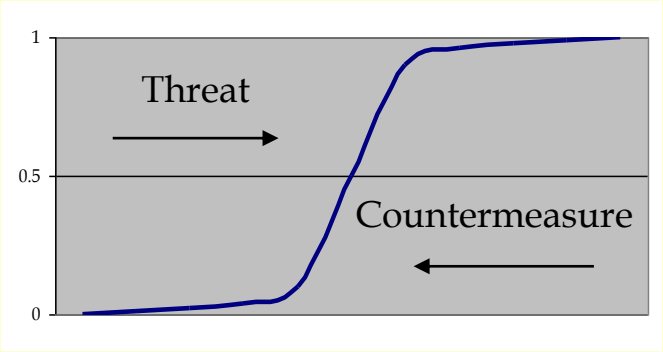
- Consider an analogy, a castle under siege from a field of archers.
- In theory, if I knew everything I needed to know:
  - About each archer (how strong he is, how tired, how steady his aim);
  - The distance between each archer and the castle;
  - The weather;
  - The lengths and weights of the arrows;
  - The characteristics of the bows, etc.
- I could work out the trajectory of each arrow and where it was going to land and whether it was going to strike the castle wall on stone or go through the arrow loop.
- I could repeat the calculation for the whole field of archers, and work out the rate at which defenders would be harmed.

How To Move Forward?

- In principle, the deterministic approach might be right. But in practice, it is simply not tractable.
- Look at how economists model the effects of an interest rate hike on inflation within the UK economy. The deterministic approach would have us model how each of 60 million people and companies would respond to the hike and summing over the lot.
- Econometrics models instead take a macro, system level, non-deterministic approach:
  - They look at the system as a whole;
  - They model the relevant characteristics in the form of distributions within the system;
  - They describe how economic influences propagate through the system and what impedes those influences;
  - They measure the outcomes in terms of economic indices and their probabilities.
- This represents a very different way of thinking. Perhaps obscure and unintuitive?
- The theory is well developed and has been very well tested and validated.
- Models are now very complex and sophisticated, and achieve considerable success.

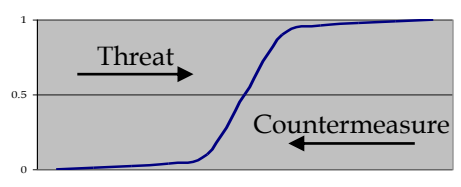
Threat-Based Security Engineering, TBSE

- It has been suggested in the past we should look at applying these types of non-deterministic technique to modelling Information Security outcomes and risk.
- This has now been attempted, and the result is Threat-Based Security Engineering.
- TBSE models the interactions between threats and countermeasures in a way which allows the likelihood and characteristics of security outcomes to be determined as a direct function of the security measures employed.



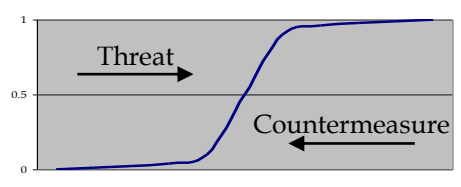
- I have found no evidence to suggest that we have been able to do this before, which makes this development very exciting.

Threat-Based Security Engineering



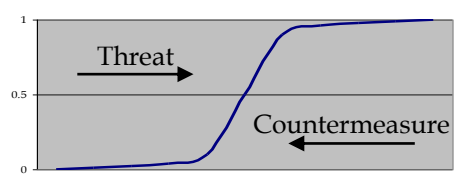
- This is very exciting. With TBSE we can:
  - Show the benefits of security countermeasures in an objective quantified form;
  - Scale countermeasures to maintain a constant level of protection in the face of changing threats;
  - Optimise security programmes to achieve required security targets whilst minimising cost, usability, complexity, performance, etc.
  - Demonstrate to stakeholders that the company's security arrangements are fit for purpose; not only effective but also efficient, reliable, verifiable.

What Stage is TBSE at Today?

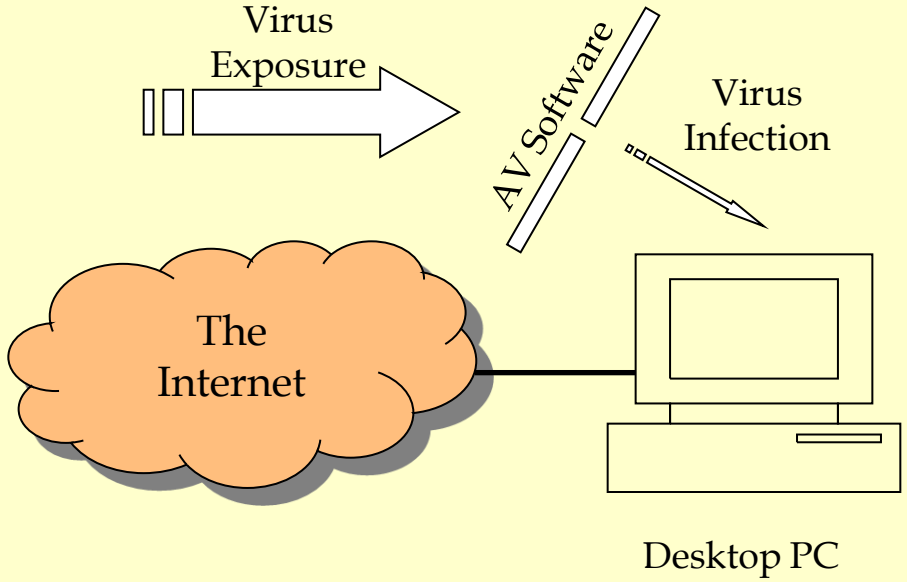


- It took years to develop complex and sophisticated econometrics models. It will take some time to develop comprehensive corporate risk models.
- The first stage is to apply TBSE to well-defined, well-bounded problems:
  - The virus threat and the use of anti-virus software;
  - The worm threat and the use of software patching;
  - The hacker threat and the use of firewalls.
- These are generic external threats. TBSE can also be applied to the generic internal threat:
  - Unintentional staff security errors (countermeasure = education and awareness training);
  - Intentional unauthorised use of privileges (countermeasure = a strong security culture).

Examples of TBSE's Results

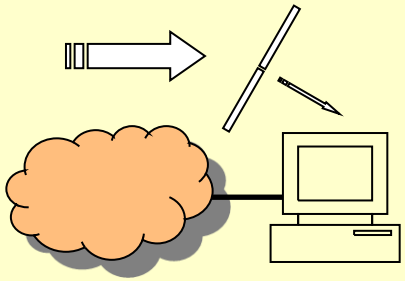


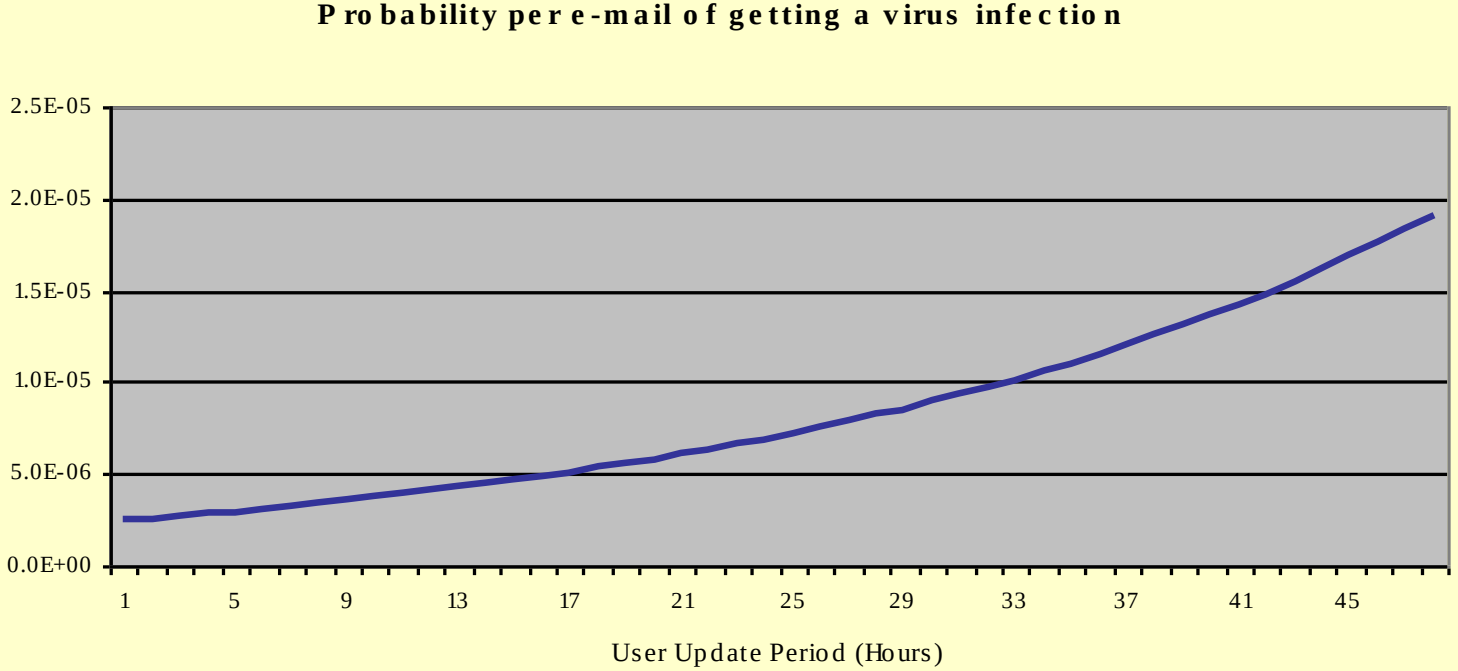
- To show what types of result TBSE can generate, we'll start with a simple and familiar scenario:
  - An Internet-connected desktop PC protected against e-mail viruses by AV software.
  - The aim is to calculate the rate of infection from a given level of threat (exposure) as a function of how well the AV software is deployed



Examples of TBSE's Results

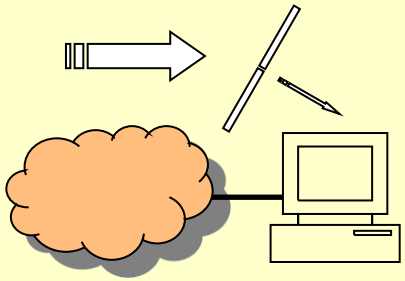
- TBSE shows how to measure the threat and describe the countermeasure analytically.
- The result is the probability (per e-mail) of my getting a virus infection as a function of the time it takes me to get new virus signatures into my user signature file.

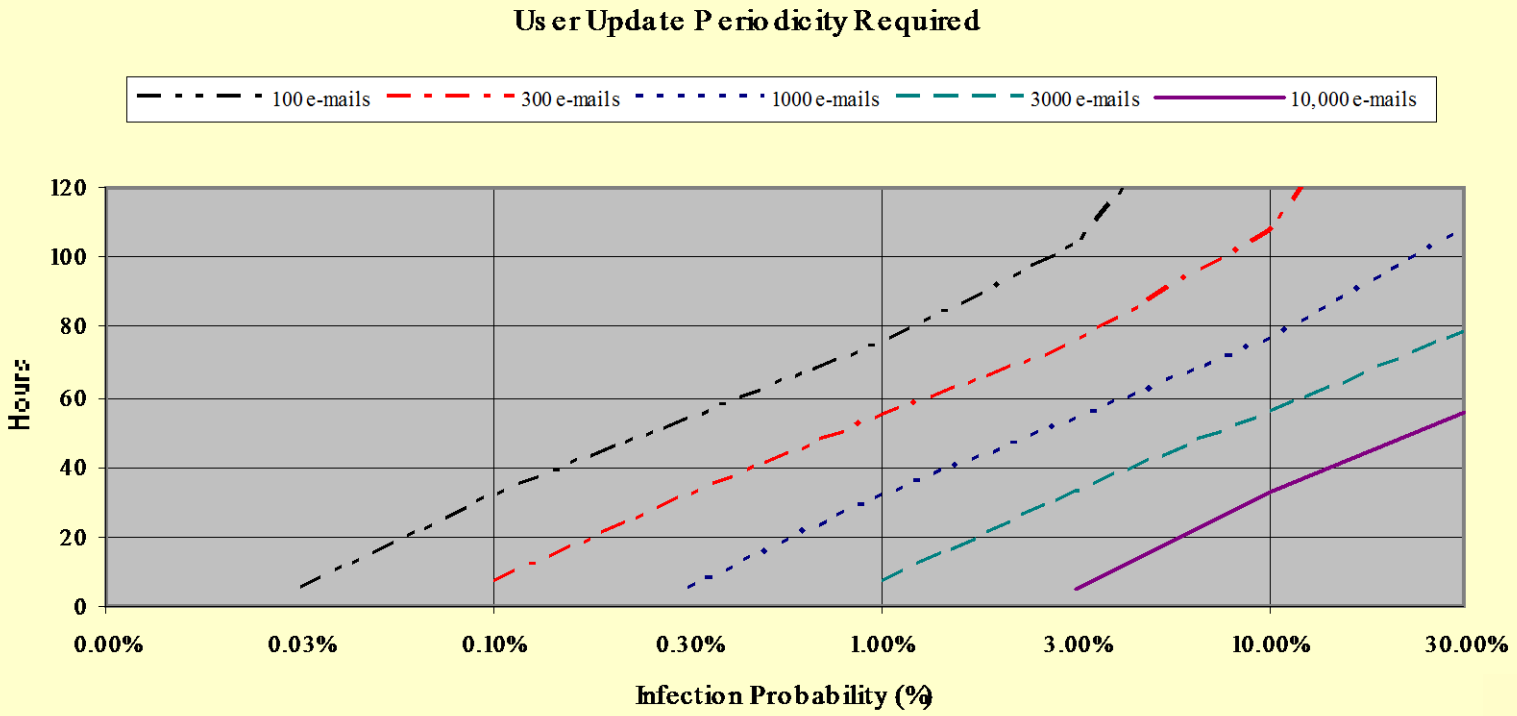




Examples of TBSE's Results

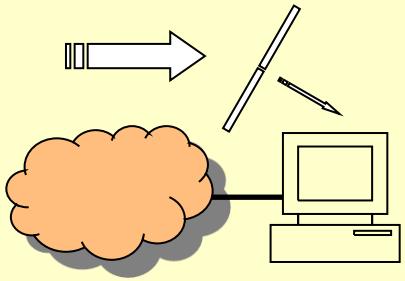
- A more useful form for the data is to show the probability of my getting a virus infection as a function of the number of e-mails I receive.



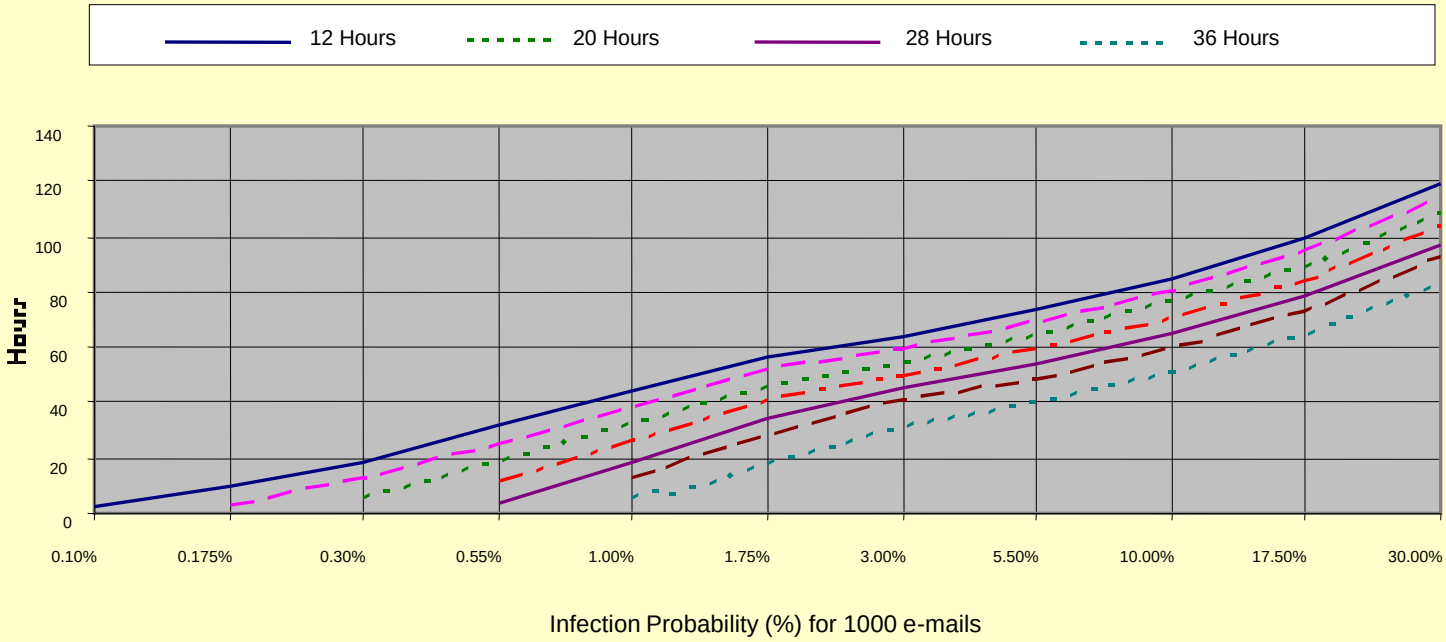


Examples of TBSE's Results

- Another potentially useful form for the data is to show the effect of changing to an AV vendor with a track record of posting new virus signatures more rapidly.

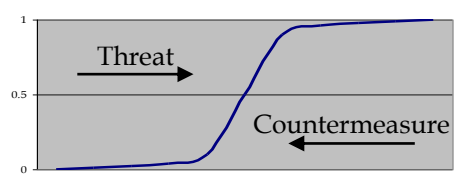


The Effect of Different AV Vendor Posting Periods

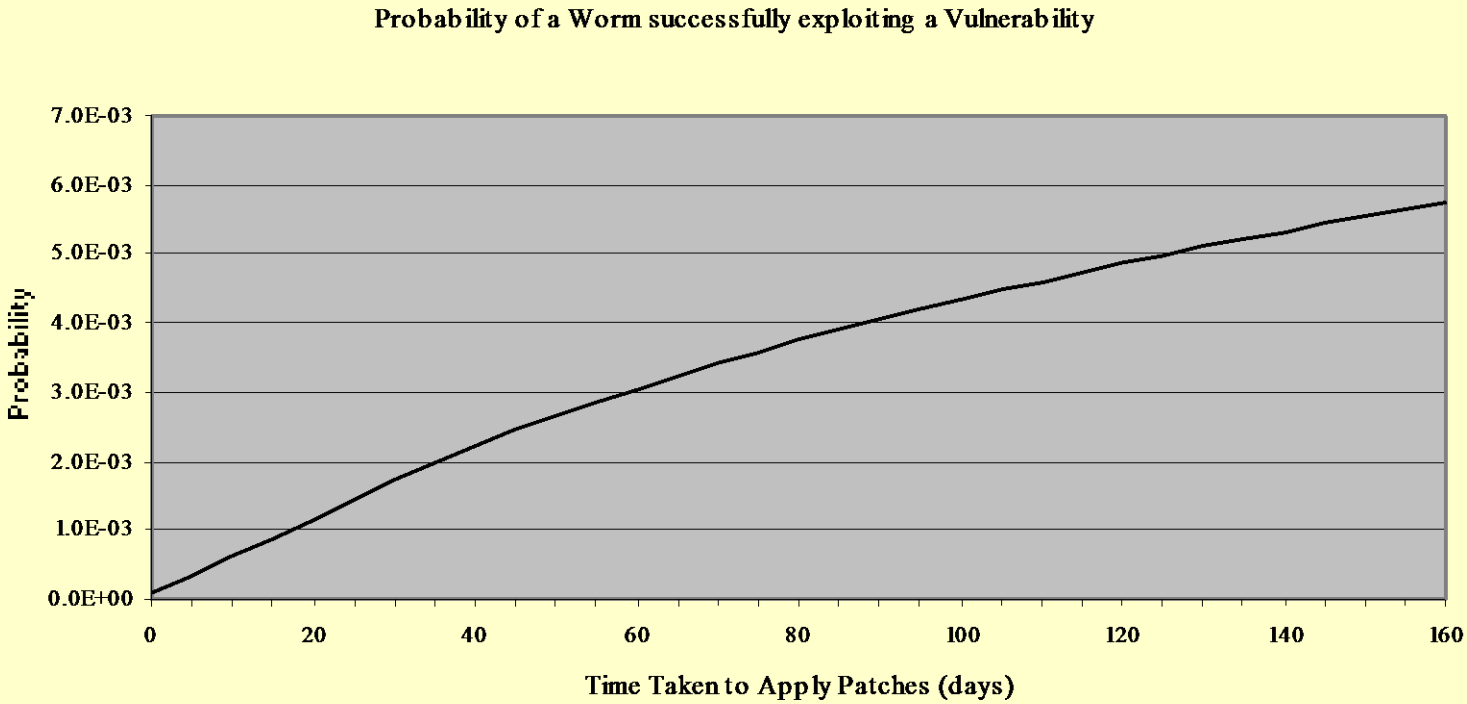


Information Security

Examples of TBSE's Results

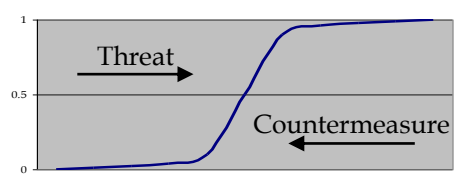


- The second example is applying TBSE to look at the benefit of software patching to protect against worms.

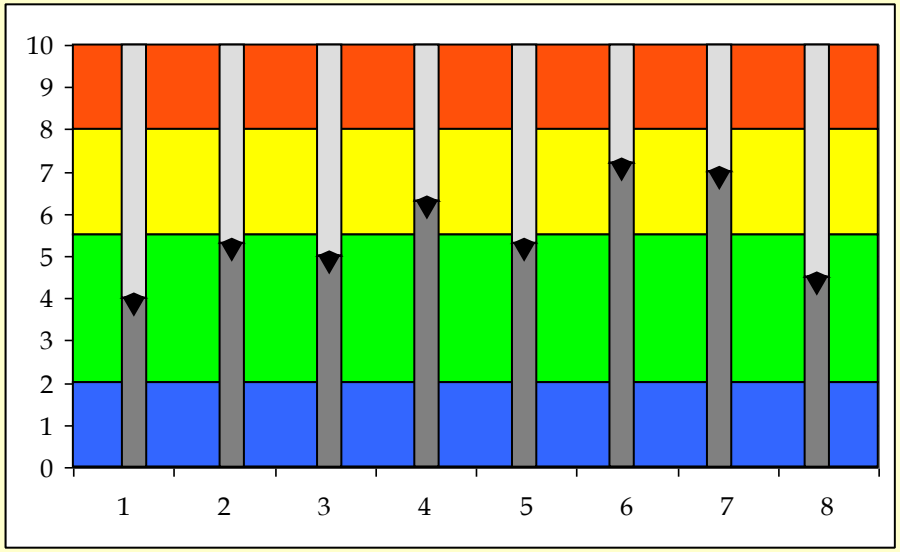


Information Security

The Next Stage for TBSE

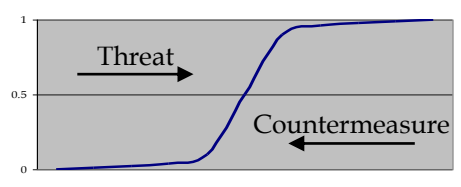


- The next stage will be to apply TBSE to more complex scenarios:
  - A single threat and several countermeasures working together;
  - Several related threats and several related countermeasures.
- Threat and Risk Barometers
  - Measure the top threats each month;
  - Measure how effectively each countermeasure is being applied;
  - Forecast the top risks over the next 3, 6, 12 months;
  - Adjust countermeasures accordingly to maintain the risk within acceptable tolerances; too high is bad, too low is bad too.



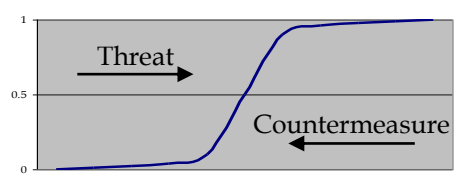
Information Security

The Next Stages for TBSE



- Beyond that, we can anticipate:
  - New products such as Digital Risk insurance products which are simple to administer and can be priced reliably;
  - New services from the providers of threat profile data and threat indices;
  - New services from management consultancies, security assurance providers;
  - New software products and management support tools.
- It has taken us many years to understand how to model risk in an analytical way.
- Now it seems we might be able to do that, there are many opportunities for applying these techniques to address long-standing problems and to improve the way we practice Information Security today.
- I believe this will allow Information Security at last to move on to become a modern engineering discipline with sound scientific roots.
- Opportunities abound for those with imagination and a willingness to innovate.

Summary



- Within the Information Security industry, we have been attempting to model and quantify risk for many years, to take out the guesswork and add some rigour to this Dark Art of ours.
- Most past analyses have taken what is known as a deterministic approach to security incidents. It turns out that deterministic approaches are simply not well suited to solving this type of problem. They have failed to deliver.
- TBSE shows how to apply non-deterministic techniques to modelling security risk and to forecasting security outcomes as a direct function of the security measures deployed.
- The impact of us now being able to model risk analytically will be felt across all areas of the field. This will bring opportunities for new services and products to be developed, 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