NCC Group Webinar

4 secrets to a robust incident response plan

(February 2015)

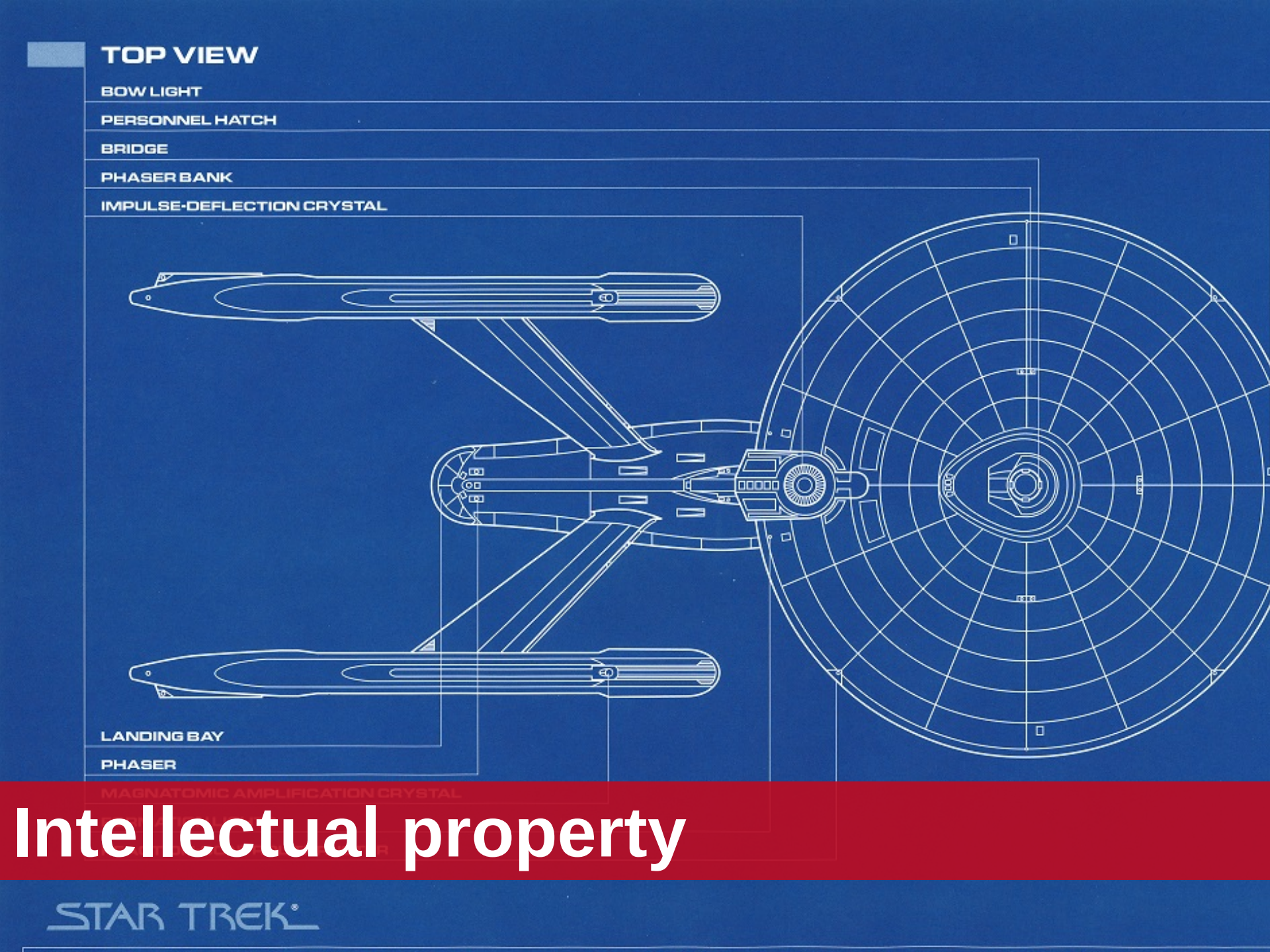
Why do we need to plan?

- **Public reporting about breaches increased again in 2014**
  - Public reporting is often about theft of credit card information, but incidents are wider than this.
  - Much of this reporting is from the USA, a very different regulatory environment.
  - NCC Group experience shows the increasing trend is relevant in the UK too.

- **Planning enables an efficient response to all types of incident**
  - From the loss of a laptop to a sophisticated targeted attack, the overall response process will follow a similar procedure.
  - Handling incidents is part of dealing with overall business risk – oversight should come from the board level.

What is at risk?

Personal information



Intellectual property

Strategic business information

Financial loss

Reputational damage

Four key considerations

1 – Don’t panic, plan!

- **Formulating a plan increases the chances of a positive outcome**
  - Enables an organisation to respond more quickly.
  - Ensures that there are no obstacles to an efficient resolution.

- **Incidents happen all the time, some are (unfortunately) successful**
  - Investment in the entire security lifecycle will reduce the likelihood of a successful attack by “raising the bar”.
  - Technical solutions cannot prevent all incidents, so prepare for common scenarios and regularly test your plans.

Case study

2 – Empower staff

- **Empower all staff by default**
  - If educated about security, staff can become an effective anti-malware solution!
  - A positive culture and response to potential incidents will encourage early reporting by staff.

- **Identify key individuals responsible for incident response**
  - Who is managing the incident for your organisation?
  - Who has authority to make decisions? Does your CEO really want this responsibility at 3AM?
  - Who will pull together internal teams who don't normally work together?
  - Do these people know when incidents should be escalated?

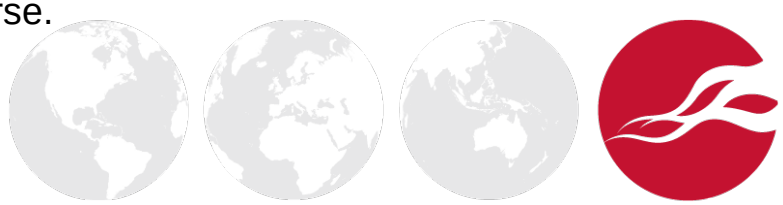
Case study

3 – Retain specialist support

- **Have relevant external specialists available on retainer**
  - You don’t want to be comparing suppliers whilst trying to deal with the reality of an ongoing incident.

- **Consider legal privilege**
  - Not always relevant or required, but useful in some circumstances.
  - Talk to your legal counsel to decide if this is appropriate.

- **This should include assistance with PR or communications**
  - Companies sometimes have an excellent technical response to incidents but communicate poorly – this can make things worse.



Case study

4 – Retain relevant data

- **Good plans can be thwarted if there is no data to investigate!**
  - Data needs to go back far enough and be readily available to investigators.
  - Consider internal applications too – is audit information available?

- **Consider how this affects third party suppliers or managed services**
  - Contracts will often include security or access to data but many suppliers are not used to clients exercising this.
  - Check whether suppliers really can help, in the same way you would test disaster recovery procedures.

Case study

Conclusion

- **Preparing is not a replacement for good proactive security investment**
  - It is always better to stop incidents from occurring.
- **Planning for an effective response does not need to expensive**
  - Consider risks and make decisions prior to an incident occurring.
  - Consider simulating an attack against your company to test how well staff and processes work.
- **Learn from incidents**
  - Review the four steps and implement improvements where required.

nccgroup
freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Milton Keynes

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney