INFLUENCING COMPANY BOARDS

June 2013

Purpose

This document has been produced to inform those who need to influence board-level decision making. It is based on the experience that CPNI has gained from briefing management boards on cyber threats and the need to consider these as part of corporate risk and business decisions.

Background

Research estimates that the cost to the UK of intellectual property theft and other online crime is likely to be in the region of £27bn¹ per annum. Commercially sensitive information, research and development (R&D) data and client details are all very attractive economic targets. In 2011 the UK Government committed to spend £650m under the National Cyber Security Programme over four years to increase the resilience of the UK to the cyber threat.

Why do you need buy-in from the board?

Our experience and many studies of cyber security undertaken indicate that getting commitment and buy-in from a company board is crucial to the successful outcome of any cyber security work. The damage that can be caused to a company by a cyber-incident is potentially huge – big enough to threaten the existence of a company in some instances. And dealing with it is also huge – it is not something that can be consigned to the IT department and promptly forgotten. Yes, tough decisions have to be made about IT security, but they also have to be made about personnel practices (is a company going to authorise the use of company laptops overseas in spite of the risks?) and about major business decisions (has the board considered the risk of espionage in setting up its new design centre in high-threat countries? Are those risks proportionate to the benefits?).

In our experience, if the board is not signed up to work on cyber security, if you do not have top-level involvement in the issue, getting truly cyber-secure becomes a greater challenge.

Getting a foot in the door

There is no set formula which gains the board’s support. To achieve a successful outcome it is important to gain a clear understanding of the board’s understanding of the threat and of their risk appetite.

Appreciating why the board might find the issue of cyber security difficult to understand and to
tackle is a significant part of a productive working relationship. The first question a board will ask
is: What impact will this have on my organisation? Impacts fall into a number of categories:

- Short-term financial – the loss of potential profit coming from a deal as the result of a hostile
foreign state knowing the negotiating position of the company as a result of the theft of
commercially sensitive information;
- Long-term financial – as above, plus the loss of profit due to intellectual property being stolen
and exploited by a hostile foreign state;
- Reputational – particularly significant for companies which rely on their reputations for
survival (for example law firms, PR companies);
- Legal – a company might fail to comply with laws such as the Data Protection Act if its
networks are compromised and data stolen.

It is crucial when talking to a board that you answer this question. It is very difficult to know how
much a cyber-security incident might cost a company (i.e. what the financial impact might be).
The following may be useful when helping boards understand the issues:

- Case studies of compromises relevant to the business which demonstrate the possible
implications on the economic prosperity or reputation of a company following an attack.
There are a number of these in the public domain, which can easily be found if you search the
internet.
- A good understanding of why a particular company might be a target of state sponsored
espionage; providing information regarding the political, military or economic interests
of some states often helps explain to a company board why their company is likely to be of
interest.
- Information regarding the extent, nature and consequences of the problem. Again, there are a
lot of resources on the internet that will help with this, with information being available that
has been produced by the public (particularly the US) and private sectors.
- Try to ensure beforehand that you have pre-briefed some member(s) of the board and that
they support what you are saying. It is extremely useful to have someone else who supports
what you are saying!
- Stay away from purely IT issues. Cyber security cannot be implemented effectively as an IT fix,
so it is important to talk to the board about tackling the problem holistically, taking into
account physical and personnel aspects of the threat.
- Cyber security should be seen by the board as a risk to the on-going success of the
organisation.

Gaining credibility

Being open and honest about the risk and providing evidence-based information can help you get
to board level – and it is vital when talking to board members. To be credible, you need to be
informed about those aspects of the organisation that are important to it. Never go into a board
briefing without researching the following about a company:

- how they make a profit (this is critical);
- company history and structure;
• whether it has Intellectual Property (IP) or undertakes Research and Development (R&D) and how important this is to the organisation;

• who their customers and suppliers are;

• how open they are, e.g. Universities have a culture of sharing information very widely;

• the extent to which their business model involves Mergers and Acquisitions;

• what international interests they have and where. Are these international interests in technologically aware countries that might have a different perspective on what legitimate business practices are?

• understanding key personalities of the board members and their backgrounds. You need to talk to them in the language they understand so you need to understand what interests and concerns them.

**Engagement with others**

Sharing information with peers is extremely useful in cyber security. Cyber is a relatively new, but prominent, security threat, and by pooling knowledge all organisations end up with a better understanding of it. Some industry sectors meet regularly to discuss security issues. Such forums enable organisations to better understand the threat, to better understand how other organisations are managing that threat – and how other boards have responded to it. Keep up to date with technological progress as well as media reports on the subject; as cyber security becomes better known, more company boards are likely to be responsive to the threat.

Industry Information Exchanges and collaboration events can help to spread the understanding about who is doing what in a sector with regard to protecting against cyber-attacks. Co-operative information sharing can raise companies’ awareness on the evolving cyber threat and increase knowledge on mitigating cyber risks. Understanding the problem holistically, and getting testimonies from peer companies, generates interest amongst board members which can influence them to consider cyber risks at an enterprise level.

External influences on an organisation’s cyber security which no business can choose to ignore (as in some cases they risk a form of penalty) are those such as legal obligations, e.g. the Data Protection Act (DPA), Sarbanes-Oxley Act or regulatory authorities such as the Financial Services Authority (FSA). The DPA legally obliges organisations to protect their personal data and the FSA requires its members to conform to financial risk management principles, which can either directly or indirectly help to improve their cyber threat awareness, and reduce their risk of cyber-attack.

**External influence**

Influential messengers such as government ministers or BBC news reports are a useful way of gaining credibility and access. Make use of publicity generated by ministers and senior security personnel. Many senior ministers are very engaged about cyber security and regularly talk about it to the media. Citing these figures can bring with it credibility and evidence that the scale of this problem is such that it is being addressed at the highest levels of government.

In addition to government pressure national and international conferences can have significant impact on the most senior members of staff. A major UK telecommunications company
responded directly at board level to the World Economic Forum’s *Global Risks 2012*, by introducing a £20 million cyber security programme following the CEO’s attendance at the conference in Jan 2011.

**Have a plan**

As with any problem presented to company seniors, it is essential to propose solutions to the issue; the point of trying to gain traction with the board is to seek the agreement of the Executives to implement the policies or processes which you believe are needed. Having an enterprise risk management strategy which identifies, assesses and, where possible, reduces the risk is a vital part of dealing with the problem. As the threat is continually evolving, a regular review of the risks is fundamental to ensuring the threat is mitigated as much as possible. People, processes and technological aspects all need to be included to provide the overall picture.

**10 steps to cyber security**

The Government has published a number of products designed to help organisations reduce the risks of cyber compromise. For example, the department of Business Innovation and Skills (BIS), GCHQ and CPNI recently launched the *10 Steps to Cyber Security* which is specifically designed to help personnel at all levels within organisations understand the issues and develop a mitigation plan.

**Further information:**


CPNI website: [www.cpni.gov.uk/](http://www.cpni.gov.uk/)


---

3 People, e.g. staff insiders, lack of awareness and/or training, lack of control (or no) user access rights.

3 Processes, e.g. prioritising the most important assets, creating a comprehensive risk profile, ensuring regular communication is effective throughout the organisation so that all staff are aware of the risks

4 Technological, e.g. regular patching, encryption, regular anti-virus software updates