MIS TRAINING - CISO EUROPE 13TH ANNUAL SUMMIT
11 – 13 MAY 2016
COPENHAGEN MARRIOTT HOTEL, DENMARK
'SECURITY RISK & GOVERNANCE:
GAINING BOARD AND STAKEHOLDER BUY-IN'
BY
LADY OLGA MAITLAND,
CHAIRMAN, COPENHAGEN COMPLIANCE UK LTD.

Slide 2. Agenda

- Can a company Board afford not to have you amongst the other board members?
- New Board trends
  - IT Committee, Cyber Security Committee, Data Committee
  - Unprecedented' demand for CIOs/CISOs to serve as a director on the board.
- The spur: Global cost of cyber attacks

Slide 2. Introduction and Lessons learnt

A CISO'S place is on the main board!

Who says so? Dido Harding, CEO Talk Talk.

- Loss of £60m due to hacking and loss of customers and reputation.
- Three attacks in 10months.

Speaking to the House of Commons investigative committee she said,
"Don't delegate security – it's a board issue and a business issue.'

The fact is the company had had two previous attacks in 10 months; no -encryption, -authorisation, -intrusion detection, -audit trail, and so on.

- They had been warned to do something but failed to act.

At a meeting recently Grant Thornton accountant's senior partners stressed their frustration at the lack of engagement by the Boards to security executives.

A meeting of the UK Treasury Select Committee had the chairman Andrew Tyrie called for a designated Board Member to take responsibility for IT security. He said referring to recent banking breaches at HSBC, Barclays, RBS 'Businesses are suffering. We cannot carry on like this,

Slide 3 a changing role of a CISO and Cyber Security is a moving target

Reality: all IT and data information are at risk. If you have got it, someone else wants it.

However, it is evident, that outside this conference, many sectors of the economy are not taking cyber security – and IT security as a whole seriously enough.

Today's leading businesses – be it SMEs or those embracing the international marketplace, handling increasing volumes of customers data – are still sidelining those responsible for protecting their precious crown jewels.

One problem being that information security has not been historically addressed as a business issue, but instead delegated to the IT department.

HOWEVER;

- Companies are now waking up to the massive consequences but often only after a major hit.
- The leak of a client's negotiation strategy is enough to severely damage any bank or law firm,
    - Just as the theft of a customer database could destroy trust irrevocably.
- Companies must get their priorities right on IT and data security = raising this to senior management level, and hire the right skills

Slide 4. The Role of the CISO'S is changing- Globally

It has never been a better time for a CISO to be heard – he is indeed a VIP and should be on the Board.

- Can a corporate afford NOT to have a CISO on the Board?
- The CISO is now seen to be part of a company's business and risk management.
- Some companies already taking a lead, e.g. Credit Suisse China

    - Asia: 60% more likely than Europe to have a CISO at Board level.
- Leading head-hunters Heidrich Struggles are now seeing as an 'unprecedented demand' for CIO/CISOs to serve on boards.
- Leading US law firm in Washington, Clifford Chance said, 'Boards don't feel they have the expertise to draw upon. They don't want to blunder into a disaster, so action has to be taken.'
- A company like Walmart has a CISO on their board.
    - As Walmart Board member Pamela Craig said, 'you need people with direct first-hand experience in the boardroom.'

Not surprisingly CISO's salaries are rising.

- The right expertise and background are commanding ever higher salaries. In the US large corporations have recently hired CISOs at between $500,000 and $750,000 with generous equity grants that have reached as high as $2m

SO HOW DOES A CISO GET THE BOARD TO BUY INTO THIS?

- A CISO now has strategic responsibilities. More business focussed,
- Understanding the mindset of the CEO, He has to think like a CEO,
    - He has to understand the way massive investment decisions are made
    - Communicating with shareholders and investors.
    - Must be able to persuade the Board that to protect their product means serious investment.
- A CISO is now part of strategic planning, risk assessment overall, and in short emerging as a business enabler, not an impediment.
- The pressure is coming from the shareholders, customers, and regulators.
- A cyber risk is equal to a financial risk and equally damaging.

WHERE A CISO IS NOT on the board, he needs to work in close collaboration with the CEO and with direct access.

- Things go wrong when The CISO is too far down the chain, with weak links to the top, and good reason to remedy this when risks have risen substantially

Slide 5. Outlook for 2016

The scale of attacks 2016 – expect a new wave.

- In financial terms hard to say how much lost, companies do not like to admit a breach, but the new 2016 EU directive forcing publication of breaches will change that. In line with the USA.
- In the US that companies are increasing the size and budget of their security teams. E.g. by the end of 2014, JP Morgan, who had been grievously hit, increased their annual cyber security budget to $250m with a staff of 1,000. In 2012, the number was 600.
- BT in the UK with already a staff of 2,500 in security are hiring another 600 this year, 2016
- Cybercrime knows no boundaries.

A review on cyber-attacks in 2016 so far. Globally

- Health insurance giant in the US Anthem
- US Florida-based 21st Century Oncology – over 2m patient's records and bank account details compromised.
- Central Bank of Bangladesh - $80m could have been worse if a spelling mistake had not been spotted in Sri Lanka.
- Europe: Europe lost an estimated 243billion Euros in Security Breaches 2015
  - The UK lost £172b.
  - An underestimate as companies does not wish to advertise their weakness and breaches.
- There will be a new wave of cyber-attacks in 2016.
  - But let us hope that we hear a new tune.

Slide 6. European Agenda on IT Security

- The EU Cybersecurity Strategy offers a framework for all initiatives on cybersecurity and cybercrime
  - Digitising European Industry strategy launched on 19 April 2016
  - Trust/security are key pillars of Digital Single Market Strategy
- 16 initiatives set in the overall strategy
  - Aims to strengthen cybersecurity & 5G, cloud computing, the Internet of Things, Data technologies

Slide 7. Responding to the threats

Attacks come from state-sponsored hackers and cyber criminals. New entrants are terrorist organisations – banks particularly vulnerable.

Govt departments and industries are equally affected.
Add to that military espionage, the political decision-making systems, let alone the Nordic innovation sectors such as technology and healthcare

What is becoming clear a several factors

1. Awareness that cyber-attacks hit first people, then technology. Hence more and more training – phishing
2. It means that as the scale of cyber-attacks rises, characterised by their persistence and sophistication; companies can no longer hope to shut out the threats behind an iron wall.
3. SMEs are most vulnerable. 60% go under within six months of the attack.
    a. The average cost of clean-up and recovery for a major company is $1m (according to Ponemon Institute)

Make it clear that the key is management.
It has been known that a major weakness being employees are who bribed or bullied to help attackers or those with a grudge. They can use staff unwittingly to their ends.

GETTING IT WRONG – companies can and do go bust

Eg Canadian Nortel, a telecom giant, went bust after the hackers stole some much of their IP
Share values shoot down. And in some cases, companies struggle to recover. Eg US AOL dropped 25%

Heartland Payment Systems who suffered a massive breach in 2008 with 100m customers debit and credit cards were taken, THEN, May 1015 computers stolen with all data including passwords. **Crisis!** The company sold in December 2015.

Talk Talk may well be sold for a penny.
Sony Pictures lost $100m and are still reeling.

This is in response to pressure from BT customers such as Unilever, National Australia Bank and even the Ministry of Defence. It is good business now for them. They earn around half a billion pounds in providing cyber expertise.

- Overall in the UK, cyber-crime costs us £34bn.

HOW DO YOU GET THE BUY – IN WHEN THE BOARD IS SLOW TO REACT?

Paradoxically, high profile attacks are the best enabler to get security onto the agenda. Maybe we need a few more sunken ships
Take advantage of any media coverage with public outrage as their bank account details are stolen. These are sharp awakeners.

A step forward can often begin at the water cooler, setting the scene for a more serious discussion with the Board.
Historically at Board level, there has been a lack of cyber awareness – they assume the engine room will take care…
Among employees a casual indifference – unless pushed.

Hence restricted budgets, and only grudgingly given. Drain on profits. No evidence of company development – let alone profit, that is until a major cyber-attack – with all the associated costs.

Slide 8. So how should a CISO present and persuade?

First, he must have the confidence to expect full access to the CEO. Chance encounters in the lift or by the water cooler are not good enough.
Get access to the CEO BY establishing a good relationship with his PA.
Only ask for 15 minutes.
Always end up being more. Keep everything in strategic business terms. This is after all that it is all about.

If you can persuade him to do lunch, then do.

When you do get to the Board - again

Slide 9. CISO is a Businessman & a Technician

THINK BUSINESS! No jargon.
The CISO has to learn the soft language of communication.

- When presenting the case, decision makers are turned off by too much technical data and babble.
- Boards need principles explained clearly. A short, succinct paper circulated in advance helps to establish a foundation of understanding.
- The Board's responsibility is governance and oversight. This is where YOU come in.
- They must understand the risks. Talk Talk ignored these at their peril. Other companies also.

- Tell it plainly and directly. Use other companies experiences and downfalls as e.g.
- Use analogies to explain technical concepts, i.e., Visualising the security issues, e.g., A home robbery is an excellent vehicle to convey complex ideas.
- Compelling stories, a video or experiences of other companies, good and bad are helpful.

A CISO goal is to establish trust and credibility through presentations and approaches. He must understand their approach to management.
ABOVE all a company Board is looking for SOLUTIONS – partly related to money.
What is the answer? What is the fix?
A CISO needs to think, 'What are the messages they need to come away with?'

One must be the threat, external and internal.

- Phishing is 20% or more to blame.
- More training. – At all levels.
- More investment in appropriate equipment.
- More staff equipped at a high level.
- To be radical, should a company employ a hacker, i.e.,. Poacher come gamekeeper? It is beginning to happen.
- Do not deliver any surprises.

If there are some shocks in store, have a private meeting first with the CEO and prime him, as well as any other tech-savvy board directors and non exec.
They will also help you to fine tune your message and identify the focus where the presentation should lie.

- Talk up systems which need attention, then where appropriate enhancing protection.
    - Your role is to understand their business goal. And if you do get to the Boardroom for a presentation, then recognise there is a reason: there is serious concern.
- Align the security risks alongside the business goal.
- Deliver the message that security is business and its business is a stand or fall one.
- CISO must keep in mind strategy, resource prioritisation and budgetary control.
- Be able to answer the Board question

    - How secure are we?

Management will ask

- What are the new and emerging trends?
- What is the plan today and the way forward
- How do we compare to our peers
- What are the potential gaps from the ideal?
- What are the consequences?

Slide 10. The really hard work for the CISO begins…

LEAVE MANAGEMENT WITH A SOLUTION –NOT A PROBLEM
DON'T BE A HARBINGER OF GLOOM AND DESPAIR

- Socialise the message, so that this a team story, a choir, and effort all singing together with a single purpose
- Need to map out a clear story line, so that security becomes an integral part of the strategic and operational business agenda.
- They are the hands-on managers, and you have to look at it from their point of view.
- WHEN YOU DO GET THE BUY – IN, this is not job done, this is where the really hard work begins as you redefine the CISO role

Slide 11. NORDIC COSTS & IMPLICATIONS

<u>Nordic countries</u>

Nordic Countries, Denmark, Finland, Iceland, Norway, and Sweden are targeted due to robust economies and valuable information in aerospace, defence, energy, health and pharmaceuticals, and shipping

The upside being that these countries generally a managing better than some and starting to include security-specific roles on the executive boards in the Nordic countries. But fact is;

- Norway in the last year has seen a 47% rise in serious attacks (huge oil and energy sector hit) let alone massive sovereign wealth fund.
    - Denmark 36%
    - Sweden 14%
- Finland only 3% but Ministry of Foreign Affairs shocked to find they had been penetrated.

- Of 700 Finnish companies surveyed by the Helsinki Chamber of Commerce, 53% of large companies consider internal threats are their biggest risk.
- In 2013 Norwegian telecoms provider Telenor was hit by an extensive cyber espionage campaign by attackers using phishing emails tricking even senior executives to reveal login data, emails, and commercial data, let alone co-operate with transferring money outside.
- In August 2015, Finnish international crane manufacturer Konecranes admitted theft was part of a scam which tricked a subsidiary to make unwarranted payments of up to $17.2m

Slide 12. CONCLUSION

As the expectations change on the CISO, so does the environment,

- The Board Is Looking For A New Layer Of The Security Professional With Executive Leadership And New Bedfellows.
- Accept That The Role Today Of A CISO Is Still High Roll. Rather Like A Rider On The Top Of An Elephant With A Small Stick.
- You Are Not In A Position Of Authority. But You Are In A Position Of Influence.
- The Momentum Of The Elephant, The Direction Of The Herd And The Landscape Around You, Resist When The Elephant Goes Against Your Desires,

REMEMBER WHO IS IN CHARGE
Feel confident in your task. The role of the CISO has changed. Executive leaders now see information risks as a key aspect of keeping their organisation stable, well regarded, trusted and ultimately profitable.

A study recently by Lloyds of London insurance about information risk management found that cyber risk is now considered one of the top three business risks. And with it, consequent rise in premiums!

At last senior executives CARE about information risk management, which means they need to hear the full story directly from the security leader = YOU!

Welcome to the Board!