Cyber Threats – Are you ready?

Jared Carstensen  SSCP, CISSP, CRISC, GCIH, CCISO, CCSK  
Security, Resilience & Forensics  
Deloitte  
jcarstensen@deloitte.ie  

11th October 2013
Cyber Security

Agenda

1. What is Cyber Security?
2. Why should I care?
3. What can I do?
4. Final Thoughts

“*We’re not as prepared as we should be, as a government or as a country.*”

Barack Obama, President of the United States
What is Cyber Security?
A formal definition

“The change in focus from reactive to pre-emptive intelligent security measures to address the dynamic targeted external threat to an organisation's digital assets and operations.”
What is Cyber Security?
A formal definition

“The change in focus from reactive to pre-emptive intelligent security measures to address the dynamic targeted external threat to an organisation's digital assets and operations.”

Cyber Security is defence against:

• Targeted external threats
• To your online systems and operations
What is Cyber Security?

It’s happening now

Threat evolution

• Increasing sophistication of attackers
• Commoditisation of exploitation
• “Lower barrier to entry” for attacker

Risk and reward

• Low risk (detection, capture, penalty)
• Potential for significant reward for success
• New motivations

It is a hot topic

• Intense and prolific media coverage
• High exposure for affected organisations
What is Cyber Security?
Common attack themes

Recent attacks highlighted in the media:

- Targeted
- Sophisticated
- Originate from overseas
- Involved several steps, suggesting intelligence
- Conducted over an extended period of time
What is Cyber Security?
Lifecycle / Anatomy of an attack

- Info gathering
- Initial invasion
- Asset discovery
- Asset capture
- Compromise

Fast and noisy
Slow and quiet
Cyber Security

Agenda

1. What is Cyber Security?
2. Why should I care?
3. What can I do?
4. Final Thoughts

“Last year alone, the US logged over 300,000 virus attacks on their networks and noted that organised crime now makes more money from cyber crime than any other activity.”

Professor John Williams, Director of the MIT Geospatial Data Centre
Why should I care?

Business Impact

Potential significant business impact:

• Revenue
• Financial losses
• Share price
• Regulatory
• Costs of remediation / investigation
• Brand / reputation

Sony hacks hit share price in Tokyo as data breaches undermine confidence

Sony's share price has tumbled following the hacking attacks on its TV and film unit, and its European subsidiary's website.

The breaches undermined confidence in Sony and sent its shares down more than 2% by midday Monday in Tokyo trade, according to AFP reports.
Why should I care?
Organisational response under examination

Common criticism of organisations following recent attacks regarding their public response:

- Defences inadequate
- Intelligence of attack lacking
- Executive understanding low
- Cyber priority at Board level inappropriate
- Response to attacks very slow & vague

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.
Cyber Security

Agenda

1. What is Cyber Security?
2. Why should I care?
3. What can I do?
4. Final Thoughts

“Protecting our interests in cyberspace is vital for the economic well-being of the UK and for our National Security.”

Rt Hon Baroness Neville-Jones DCMG, Minister of State for Security and Counter-Terrorism
What can I do?
Reduce the business risk

Four key priorities:
• Prepare
• Aware
• Respond
• Defend

![Graph showing business risk reduction over time and investment, with labels for pro-active threat management and re-active compliance based security.]

1. To view Deloitte drawing guides:
   2. Right-click on slide and select 'Grid and Guides...'
   3. Check 'Display drawing guides on screen'
   4. Select 'OK'
What can I do?
How can an organisation defend?

Prepare
- Defence
- Communication
- Co-ordination
- Capability

Aware
- External intelligence
- Internal intelligence
- Consolidation

Respond
- Strategic
- Communication
- Risk assessment
- Technical

Defend
- Employee
- Targeting
- Assets and risks
- Detection
What can I do?
Increasing sophisticated and determined attacker

Attacker Sophistication

Risk Appetite

Reduced ROI

State-sponsored Cyber Warfare

Organised Crime

Defend

Limit impact

Attacker Determination

Accidental Discovery

Malware

Insider

Lone Hacker / Hobbyist

Business Partner

‘Script kiddy’

Disgruntled ex-IT Administrator

Competitor

Disgruntled Customer

Disgruntled ex-Employee

Hacker Collectives

Cyber Terrorism

‘Hacktivism’
What can I do?
How does my organisation compare in maturity terms?

Situational awareness

Quality of intelligence and depth of distribution
Forensic analysis capability
Actionable intelligence

Intelligence collection
Operations
Event correlation
Protective threat planning

‘Traditional’ compliance-based IT and Network security

End Goal
Enabling Capabilities
Foundations
What can I do?
5 rules of the road for the Non Executive Director

- Challenge the board: make sure cyber security is on the board’s agenda
- Raise awareness of the business impact of a successful cyber attack
- Identify competent and aware cyber security leaders
- Ensure effectiveness of the organisation’s cyber security defences
- Provide increased senior management attention and oversight
Summary
This is real and it could happen to you

Challenge

• Organisations are facing a perfect storm of:
  • Increasing numbers of vulnerabilities
  • That are more easily exploited
  • By people more willing to break the law
• Attacks increasingly targeted
• Attackers increasingly using multiple attack routes
• It is very likely you will be subject to a successful Cyber Attack

Response

• Actionable, relevant intelligence to focus resources
• Change in focus from reactive controls to proactive preventative ones
Final Thoughts – Reckless or Asleep at the Wheel?

In the same way as there are car accidents every single day, security breaches and incidents are occurring almost as frequently. Are there similarities?

- Rules of the road to protect drivers and pedestrians
- Regulations & standards to protect organisations and consumers.
- Speed limits depending on the road type
- Regulations depending on type of business & industry
- Wide choice of cars available, depending on your needs
- Wide choice of providers and security options available depending on your needs
- By not adhering to rules of the road – you put your own, and others lives at risk
- By not adhering to security rules – you put the business and its customers at risk
- Despite all these road rules – thousands of accidents happen every day
- Despite all the regulations, standards and security awareness - countless security incidents, breaches, and non-compliance continue.

Are organisations “driving recklessly”, or are they simply asleep at the wheel?
Jared Carstensen  SSCP, CISSP, CRISC, GCIH, CCISO, CCSK
Security, Resilience & Forensics
Deloitte
jcarstensen@deloitte.ie

©2011 Deloitte LLP: The seminar and these accompanying handouts have been written in general terms and therefore cannot be relied on to cover specific situations; furthermore, responses given in the seminar to questions are based on only an outline understanding of the facts and circumstances of the cases and therefore do not form a substitute for considered specific advice tailored to your circumstances. Applications of the principles set out will depend on the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this seminar and these accompanying handouts. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this handout to their specific circumstances. Please feel free to contact any partner.
We would be pleased to advise you on the application of the principles demonstrated at the seminar to your specific circumstances but in the absence of such specific advice cannot be responsible or liable to you for the content of our presentation.