



Cyber Crisis Management Handbook

Sébastien Héon, Director Political Affairs, Cassidian Cyber security

Cyber Crisis – Are they for real?

78%	of large organisations were attacked by an unauthorised outsider in the last year (up from 73% a year ago)
39%	of large organisations were hit by denial-of-service attacks in the last year (up from 30% a year ago)
20%	of large organisations detected that outsiders had successfully penetrated their network in the last year (up from 15% a year ago)
14%	of large organisations know that outsiders have stolen their intellectual property or confidential data in the last year (up from 12% a year ago)

23%	of respondents haven't carried out any form of security risk assessment
53%	of respondents are confident that they'll have sufficient security skills to manage their risks in the next year
31%	of respondents don't evaluate how effective their security expenditure is

Source: UK government – 2013 figures

Usual targets of cyber attacks:

- IPR,
- ongoing commercial negotiations,
- emails of VIPs

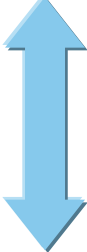
Lessons Learnt on Espionage cases (1/2)


- **371 Days**: the median number of days between the start and the detection of an attack
- **“Five stages of grief”** when an organisation faces a cyber attack:
 - Denial: “you’re mistaken”
 - Anger: “How dare they attack me?”
 - Bargaining: “Is it really a problem?”
 - Depression: not a long stage
 - Acceptance: “What can we do?”

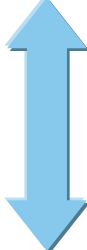
Lessons Learnt on Espionage cases (2/2)

- Internal IT Security teams are in an awkward situation...
... and we are not welcome...
- Operational procedures are lacking

Recovery

- Analyse and understand
 - Track the attacker, analyse its tools and modus operandi
 - Forensics to backtrack to “patient 0”

~3 months
- Neutralize
 - Not too soon otherwise the attacker will hide

1 week-end
- Recover
 - As attacks are becoming more sophisticated, the recovery phase is more and more time consuming

1+ year

Conclusion

- Prevention is cheaper than reaction
- Prevention is predictable (budgets, planning,...), reaction is not
- Prevention occurs before your secrets has been stolen...
- Solutions exists to avoid cyber crisis

“If you think education is expensive, try ignorance”
Abraham Lincoln

Thank you for your attention!

Sébastien Héon

sebastien.heon@cassidian.com

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without express authorization is prohibited. Offenders will be held liable for the payment of damages.
All rights reserved in the event of the grant of a patent, utility model or design.