A HACKER'S GUIDE TO INCIDENT RESPONSE

David Stubley

WHO AM I?

- 12 years experience within the technical security market
- Experience within both private and public sectors
- Director with 7 Elements Ltd
- Key role to bridge the gap between technical teams and senior management
- Huge wealth of experience gained through high profile security incidents and security assessments

INTRODUCTION

“All characters appearing in this work are fictitious. Any resemblance to real persons, living or dead, is purely coincidental….”

CONTENT

- Context
- Experience
- Case study
- Conclusions
- Questions?

CONTEXT

Hack
Pronunciation:/hak/
verb

1. gain unauthorized access to data in a system or computer.

2. program quickly and roughly.

http://oxforddictionaries.com/definition/hack

EXPERIENCE

OCG

Hackers

APT

Media

CASE STUDY

CONCLUSIONS

- Remember that sound forensic practices need to be used in cases that will involve the local law enforcement or courts.
- Use your specialists as just that, specialists!
- Focus on what is required.
- Trust but verify!
- Remember, LOGS, LOGS, LOGS.

QUESTIONS

?

Resilient Information Security

www.7elements.co.uk