



SEGWARP

The South East Government Warning Advice and Reporting Point

Tony Osborn, Bruce Fowlie

UK Public Sector Technology Team

Agenda

1 What to watch out for - security landscape

2 Workshop on two topical areas;

Implications of outsourcing on Information
Governance

Implementing BYOD

1

What to watch out for on security landscape



Threat Landscape

2010 Trends (we saw 9 unique attacks per second!)

1

Targeted Attacks

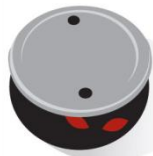
continued to evolve (Aurora/ Stuxnet)



3

Hide and Seek

(zero-day vulnerabilities and rootkits)



5

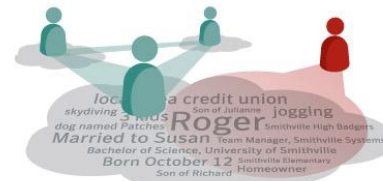
Mobile Threats

increase (up 42% to 163)



2

Social Networking + social engineering
= compromise (eg Tiny URL)



4

Attack Kits

get a caffeine boost (Java targeted kits)



<http://www.symantec.com/threatreport/>

Threat Landscape

2010 Trends (we saw 9 unique attacks per second!)

1

Targeted Attacks

continued to evolve (Aurora/ Stuxnet)

Identify your crown jewels (ie. Information), apply defence in depth using people/process/technology

2

Social Networking + social engineering

Have a policy on social networking on company devices, keep up to date on employee education

*Born October 12, 1970
Son of Richard Homeowner*

3

Hide and Seek

Establish a working patch management process, especially application patching and 'critical' system patching

5

Mobile Threats

Embryonic, have a strategy on this that meets the business needs and understand what data is actually on the devices

4

Attack Kits

Keep technology up to date (eg. AV updates) and keep your knowledge up to date on what is possible in the threat world.

UPDATABILITY ENGINE
OBFU

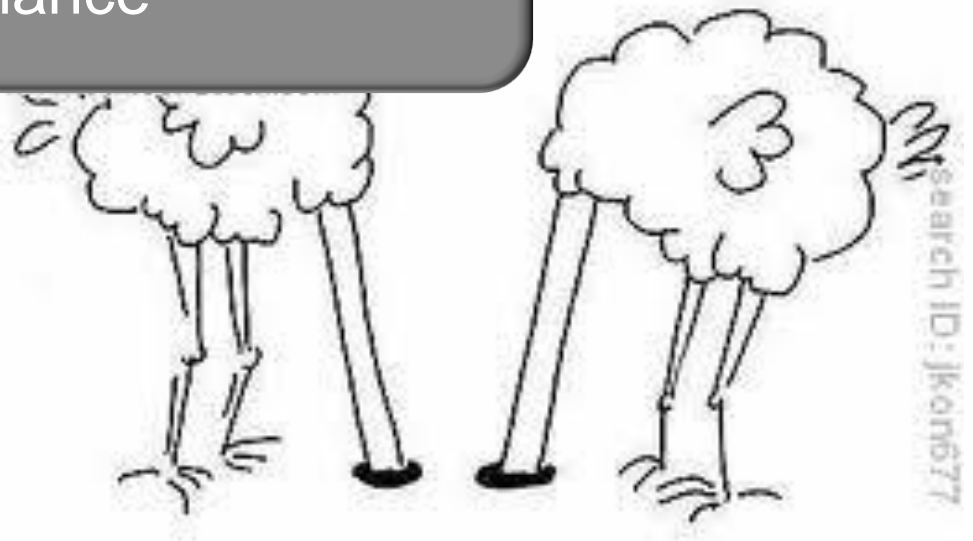
<http://www.symantec.com/threatreport/>

2

Mini - workshop on two topical areas;



Implications of outsourcing on Information Governance



"There you are!! I've been looking for you!"

Set the scene..

If we don't understand our data how can we effectively manage or secure it!.

Can you answer these questions;

- what data is more, or less, important?
- where is this data at any time?
- who owns (Controls) it?
- who uses (processes) it?
- what its used for?



If you have an fully managed outsourced IT supplier ,
who is the data Controller?

Data Protection Act

Principle 7 (P7) Security .. What does this mean in practice?

- Organisations must indentify their relationship to the data (Controller, processor etc)
- Organisations should have an awareness of technology and what is available at a reasonable cost for their organisation
- Technology must meet the needs based on the data and the harm that maybe caused if used incorrectly, lost, damaged or destroyed
- Employee cultural change required to become 'stewards' of citizen data

Take 10 minutes – how many questions do you ask of your outsourcers?

Category	Topic	Specific
Security	1. Physical Security	Does the supplier follow good practice?
	2. Personnel	Does the supplier have a policy and abide by it (e.g. ISO27001)?
	3. Access Control	Does the supplier have access control mechanisms, such as logical and physical separation of duties, in place?
Performance	4. Monitoring	Does the supplier monitor information security performance (e.g. breaches, reviews, internal SLA's) ?
	5. Security testing	Does the supplier have regular InfoSec tests (e.g. Pen test)?
	6. BC and DR	Does the supplier have a BC and DR plan? Is it tested? Is there an agreed SLA for recovery time?
	7. Reporting	Is the InfoSec performance available to the customer?
Compliance	8. Legislation	Is the supplier aware of their compliance requirements and are they providing good Info. Gov.?
	9. Certification	Does the supplier hold certifications (e.g. ISO9000, ISO 27001 etc)?
	10. Audit/review	Does SLA performance allow customer audit?

Feedback

Category	Topic	Specific	Feedback
Security	1. Physical Security	Does the supplier follow good practice?	
	2. Personnel	Does the supplier have a policy and abide by it (e.g. ISO27001)?	
	3. Access Control	Does the supplier have access control mechanisms, such as logical and physical separation of duties, in place?	
Performance	4. Monitoring	Does the supplier monitor information security performance (e.g. breaches, reviews, internal SLA's) ?	
	5. Security testing	Does the supplier have regular InfoSec tests (e.g. Pen test)?	
	6. BC and DR	Does the supplier have a BC and DR plan? Is it tested? Is there an agreed SLA for recovery time?	
	7. Reporting	Is the InfoSec performance available to the customer?	
Compliance	8. Legislation	Is the supplier aware of their compliance requirements and are they providing good Info. Gov.?	
	9. Certification	Does the supplier hold certifications (e.g. ISO9000, ISO 27001 etc)?	
	10. Audit/review	Does SLA performance allow customer audit?	



**What are your thoughts on how
you can build in greater
information governance into
outsourcing contracts?**

Bring Your
Own Device!!



I LOVE THIS THING!

Set the scene..

- Some 33% of respondents already use consumer devices in certain parts of their operational environment; 75% have pilots or trials running.

•Over 70% remarked that the pressure for increased adoption and change in this area was escalating – most saying “escalating severely”

(ISF – Securing Consumer Devices report)



Workshop

Split into 3 groups.

15 minutes discussion.

**5 minutes feedback per group,
nominate a speaker**

In your groups – how would you answer these questions?

1. What are the specific compliance (internal or external) pressures to Local Government organisations (eg. DPA Principle 7, PCI etc)?

2. How you will demonstrate ‘auditability’ (particularly in a regulated environment): eg audit trails, capacity for forensic investigations.

3. How can you separate business use and private use to reduce risk of breaching policy?

4. What key considerations are required regarding existing infrastructures?

5. What barriers exist to you encrypting all applications and data?

6. What are the key considerations when deploying anti-malware software? (eg. multiple devices with differing operating systems)

7. What are the top items to include in an Acceptable Use Policy (AUP)?

8. How do you manage the tech-savvy users?

9. What pre-work would you do with the user community (eg. User forums etc)

Compliance

Technical

users

Examples taken from ISF ‘Securing Consumer Devices Report (April 2011)

Questions and feedback?

*Would you like your workshop summarised
and fed back to you at a future meeting?*



Thank you!

tosborn@Symantec.com

Bruce_fowlie@symantec.com

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.