Incident Response

Tony Drewitt – Head of Consultancy
IT Governance Ltd
www.itgovernance.co.uk

IT Governance Ltd: GRC One-Stop-Shop

Thought Leaders
Specialist publisher

Implementation toolkits

ATO

Consultants

Software and e-learning

Distribution

IT governance, risk and compliance

Cyber resilience				Governance and risk management		
Information security and ISO 27001		Business continuity management and ISO 22301		IT governance	Service management	Project management
PCI DSS	Penetration testing	Data protection	Incident response management	COBIT®	ITIL® and ISO 20000	PRINCE2® and PMBOK®
Consultancy and certification	Security testing	Training and qualifications		Software tools		Toolkits and publications

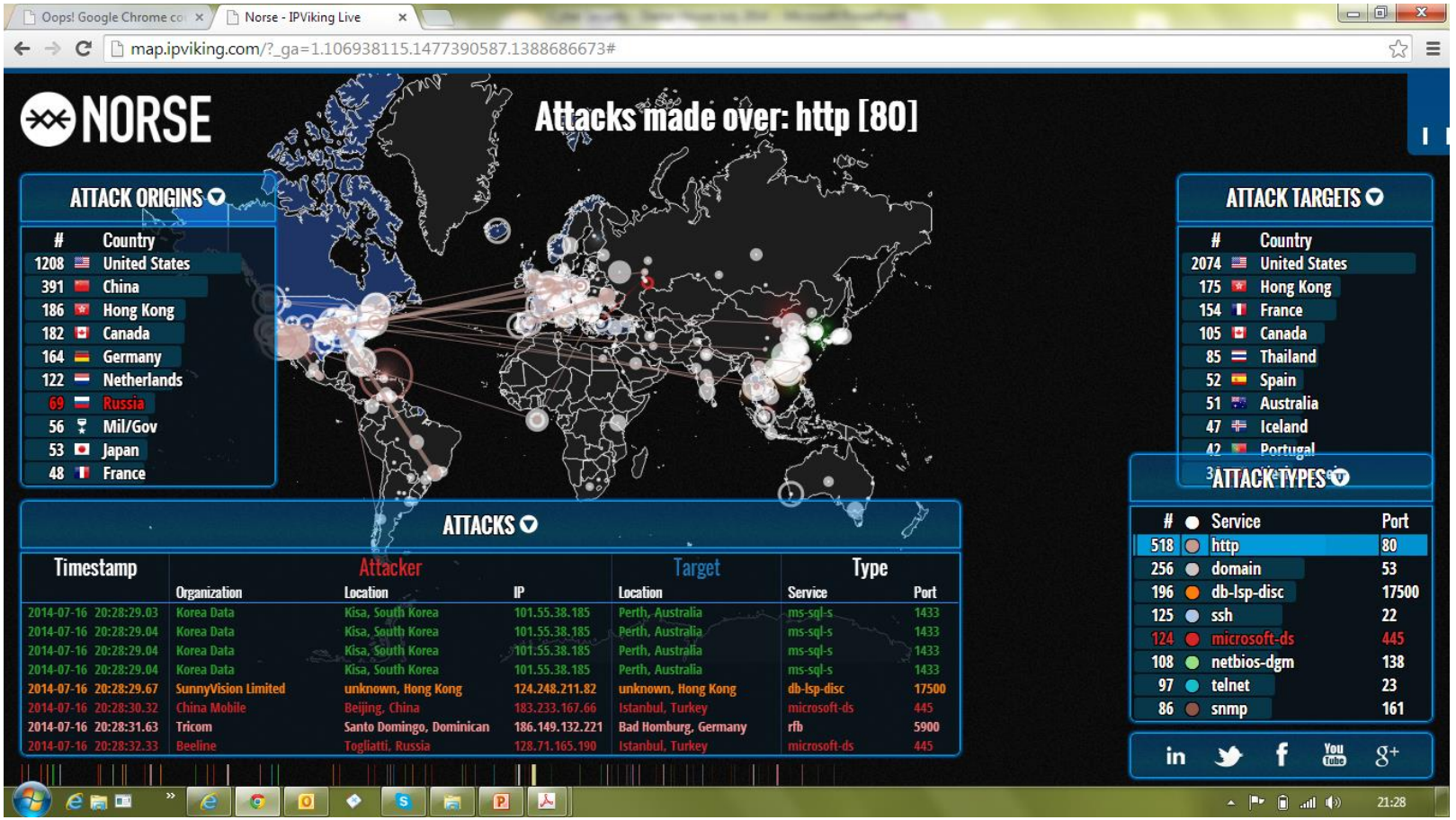
Point solutions that integrate……

APMG-International ISO/IEC 20000 · bcs The Chartered Institute for IT · IBITGQ Certifying Competence · CYBER ESSENTIALS · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CREST · CYBER ESSENTIALS PLUS · ISO 9001 CERTIFICATION EUROPE · ISO 27001 CERTIFICATION EUROPE

Agenda

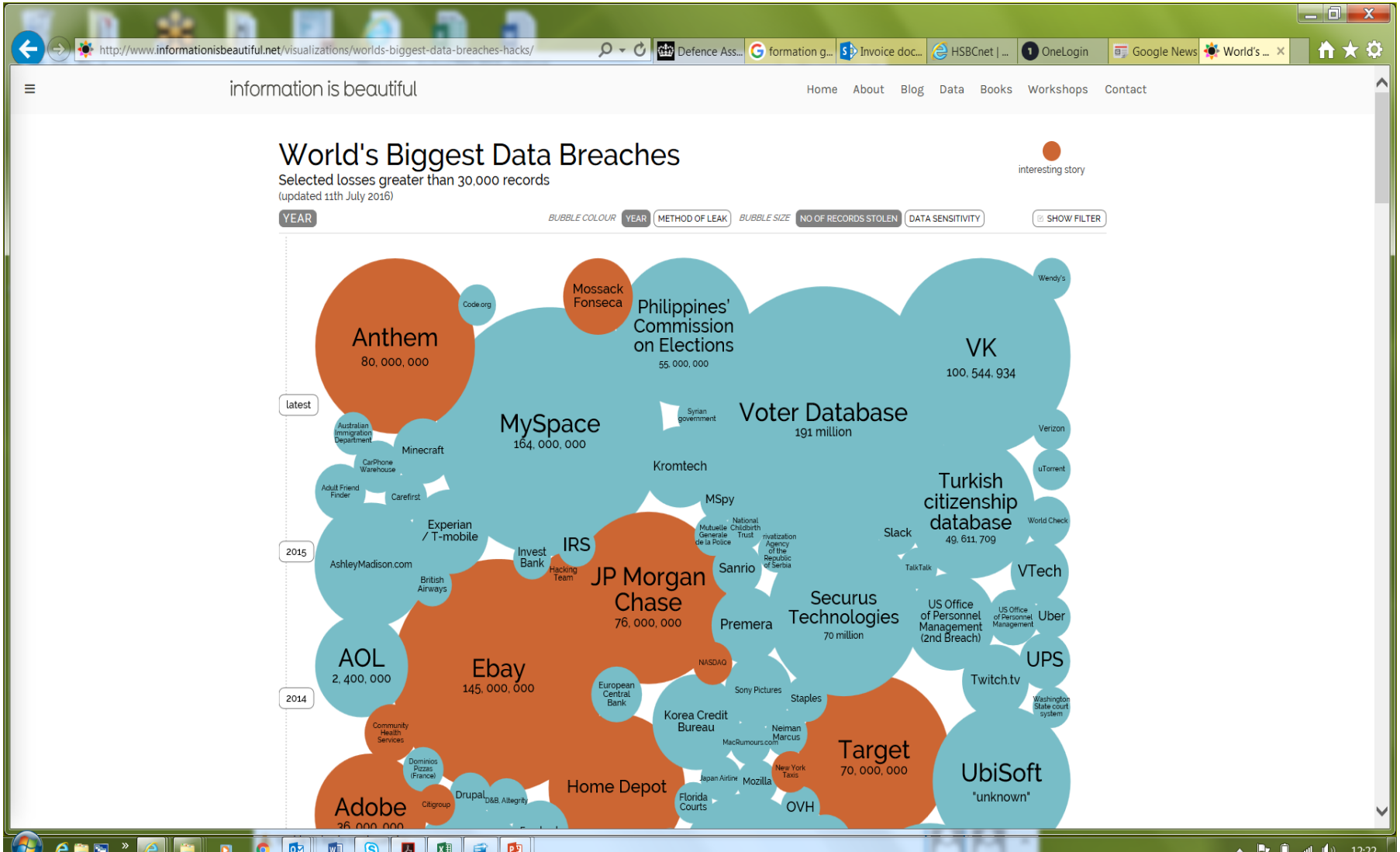
- Today's cyber threat environment
- Cyber Assurance
  - People
  - Process
  - Technology
  - Digital vs. physical security
- Resilience vs. response
- Response structure

The Cyber Threat Environment



Massive data breaches

- www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Cyber Risks for all

- Digital Information is at the heart of cyber crime
  - Key assets at risk:
    - High Value Research – e.g. energy technology, biotechnology, advanced engineering
    - Politically/commercially sensitive data – e.g. product development, climate modelling, testing data
    - Sensitive internal information: e.g. PII (customers and staff), financial data (eg bank accounts, payment card data, identity theft)
  - Key challenges:
    - Balancing openness with security
    - Devolved data management responsibilities
    - Multiple, mobile and remote access connection requirements
    - Complex data lifecycles
    - Rapid technology evolution

Security breach levels are rising

Security breach levels continue to rise. Last year in the UK:

- 90% of large organisations reported suffering a security breach, up from 81% a year before.
- 74% of small businesses had a security breach, up from 60% a year before.

Source: BIS/PwC 2015 Information Security Breaches Survey

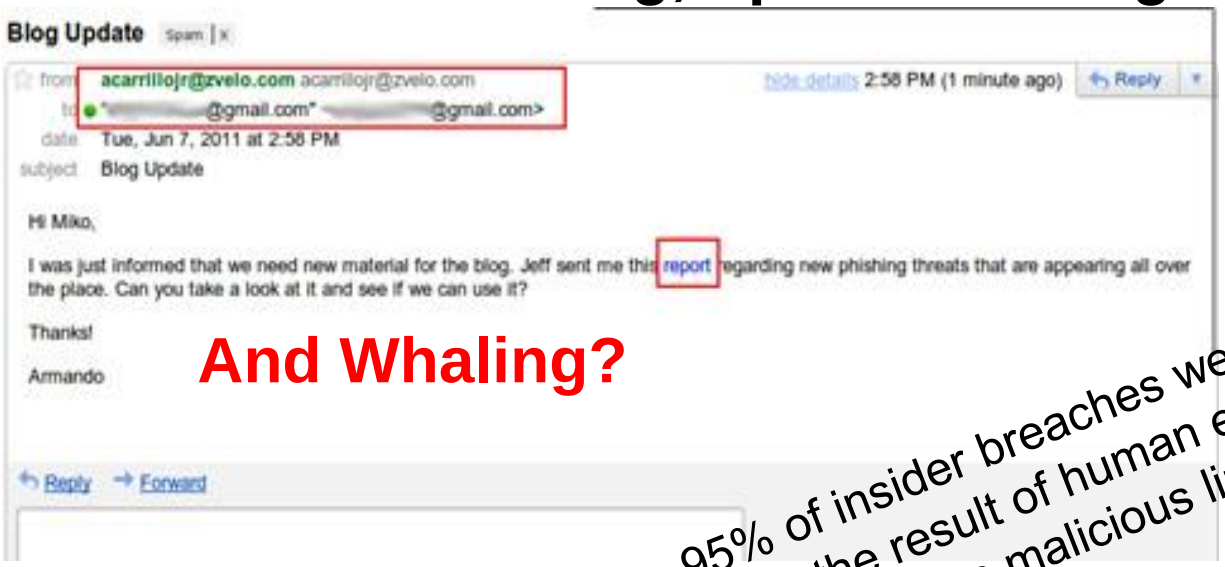
Cost of cyber crime is rising

The average cost of a data breach for businesses in the UK is £2.37 million.

Source: IBM/Ponemon Institute 2015 Cost of Data Breach Study: United Kingdom

Hacking the Human

Phishing, Spear Phishing


Blog Update Spam | x

from acarrillojr@zvelo.com acarrillojr@zvelo.com

hide details 2:58 PM (1 minute ago) Reply

to "[redacted]@gmail.com" [redacted]@gmail.com>

date Tue, Jun 7, 2011 at 2:58 PM

subject Blog Update

Hi Miko,

I was just informed that we need new material for the blog. Jeff sent me this report regarding new phishing threats that are appearing all over the place. Can you take a look at it and see if we can use it?

Thanks!

Armando

Reply Forward

And Whaling?

95% of insider breaches were found to be the result of human error, such as clicking on malicious links in phishing emails.

Small Businesses are Popular with Hackers

- Shared servers - Multiple access points for hacker exploit.
- No IT department/function - hardware and software not always up-to-date.
- Website versions and plug-ins often out-of-date - easily hacked
- Minimal/no internal security practices - passwords and access easily compromised
- Websites often built on common, open-source frameworks – common, well known vulnerabilities

Cyber Assurance

- Hackers, crackers & attackers will never “go away”
- Modes of attack & failure are many and varied
- To remain in the digital world vulnerabilities must be continually monitored
- Few organisations can afford every digital control available
- A risk-based approach is the only viable response for the majority

Risk and Appropriate Control

Risk and Appropriate Control

People & Process

- Do people make (cyber) mistakes?
- Can people be (cyber) exploited?
- Can processes include (cyber) vulnerabilities?

- Shall we assume “No”?

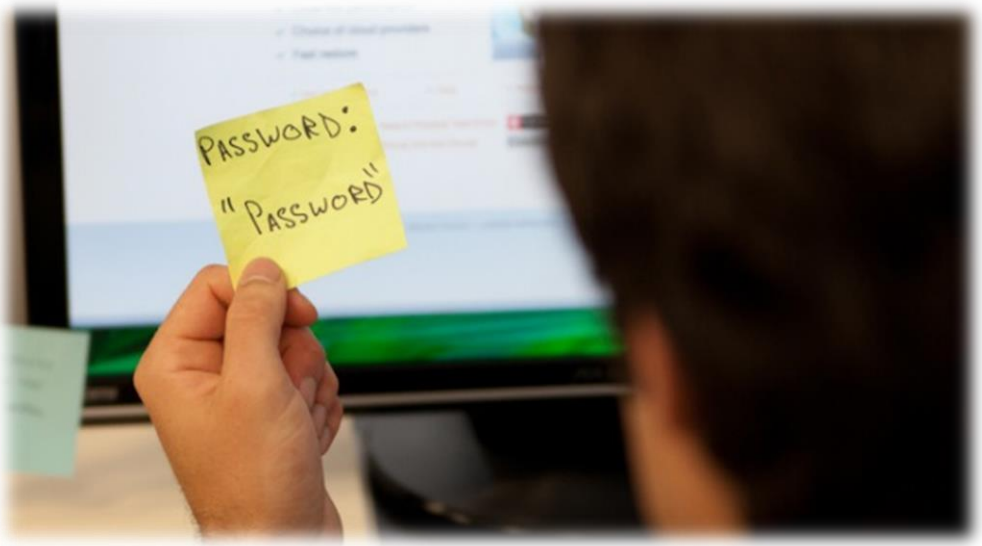
Technology

- Connection = exposure
- Which controls?
- Your recipe or a recognised successful one?

- Approved by National Cyber Security Centre

Digital vs Physical

- Does the physical environment play a role in cyber security?

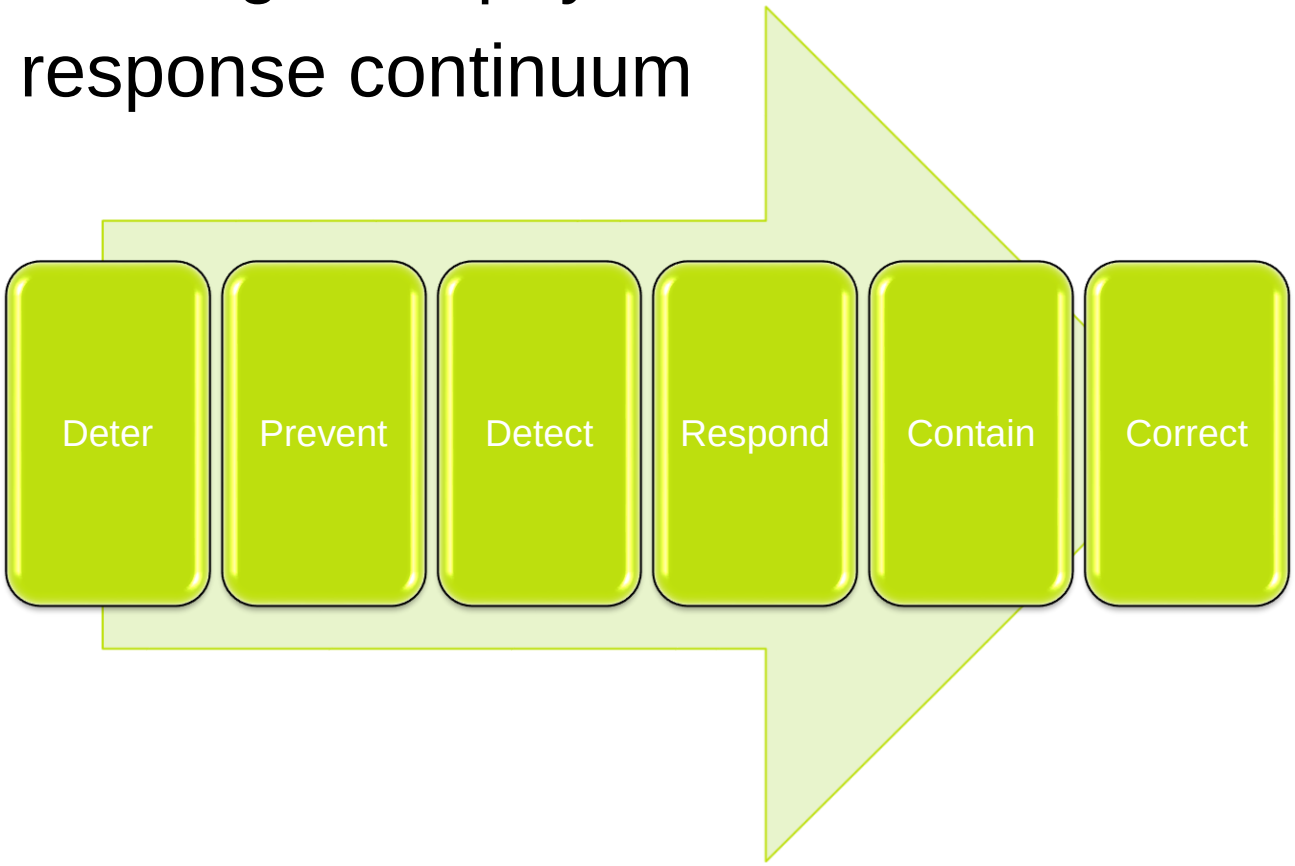


Breaches

- Consequences
  - Compliance failure
  - Loss of value
  - Business disruption
- Some controls detect & initiate response
- Business continuity plans & arrangements
  - No plan = weak response, bigger impact
  - Plan = optimal response, minimised impact

Resilience vs. Response

- 100% prevention = disconnection
- Prevention = logical + physical + human
- Incident response continuum



Breach Recovery

- Cyber security is about defence
  - Protect C, I, A
  - Respond to Incidents
  - Maintain security posture
- However – defences are being – and will be - breached…..
  - How should we respond, in what order?
    - Not part of ISO27001
    - Not part of traditional Information Security

Cyber resilience

- Business Resilience:
  - “the ability to rapidly adapt, protect business assets, respond to business disruptions and maintain continuous business operations..”
  - Contains both BCM and DR
- Cyber-resilience:
  - “the ability to repel cyber attacks while protecting critical business assets, rapidly adapting and responding to business disruptions and maintaining continuous business operations..”

Supporting Standards

- ISO/IEC 27031 - Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032 – Guidelines for Cyber Security
- ISO/IEC 27035 - Information Security Incident Management
- ISO/IEC 27036-3 Information Security for Supplier Relationships
- ISO 22301 – Business Continuity Management System

7-Step Cyber-resilience Strategy

1. Governance, clear policies, leadership
2. Business, regulatory and contractual requirements
3. Integrated risk assessment, BIA, DPIA
   - Assets AND Processes
4. Secure the cyber perimeter & endpoints; defence in depth
5. Train all staff – skills, competence, awareness
6. Develop and test a security incident response and escalation plan
7. Audit, monitor, test, continually improve

Adopt and integrate ISO27001, ISO27031, ISO27035, ISO22301

Questions?

tdrewitt@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk