

# Maintaining Information Security in an Age of Austerity

---

*An update on new risks and challenges*

---

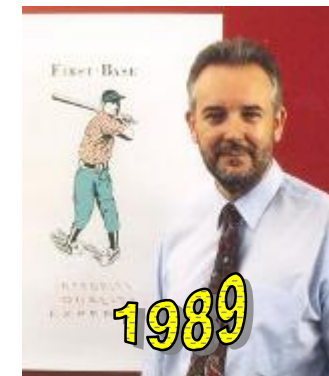


Peter Wood  
*Chief Executive Officer*  
First • Base Technologies



# Who am I ?

- Worked in computers & electronics since 1969
- Founded First Base Technologies in 1989  
(one of the first ethical hacking firms)
- Primary roles:
  - Network penetration tester
  - Social engineer
  - Conference speaker
  - TV and radio security 'expert'
  - Security author
  - Active member of BCS, IISP and ISACA
  - FPWS





# Typical Security Reviews

1. External infrastructure penetration tests
2. Remote access tests
3. External web application tests
4. Internal network discovery and penetration tests
5. Internal Windows penetration tests
6. Server security reviews
7. Database and internal applications tests
8. Wireless penetration tests
9. Endpoint penetration tests
10. Social engineering tests



# External Infrastructure Penetration Tests

- Focus only on 'live' addresses  
(simple IP scan first)
- Could be automated at lower cost  
(with reduced accuracy)
- Little preparatory work
- Provide good benchmarks
- Annual tests are sufficient  
(unless the infrastructure changes)



## Remote Access Tests

- Each external service requires testing (OWA, Citrix, extranets)
- Authenticated tests preferable (to identify privilege escalation etc.)
- Little preparatory work
- Provide good benchmarks
- Annual tests are sufficient (unless the services change)



## External Web Application Tests

- Web sites are the most vulnerable to external attack
- Authenticated sites require manual testing (cannot be reliably automated)
- Modest preparatory work
- Annual tests are sufficient (unless the application changes)



# Internal Network Discovery and Penetration Tests

- Highlight internal infrastructure problems
- Can be combined with Windows penetration tests to reduce cost
- Little preparatory work
- Provide good benchmarks
- Good indicator of IT staff security awareness



# Internal Windows Penetration Tests

- Highlight Windows security problems
- Can be combined with internal network discovery to reduce cost
- Little preparatory work
- Provide good benchmarks
- Good indicator of IT staff security awareness



# Internal Server Security Reviews

- Authenticated technical audit
- Verify build standards and configuration
- Can be combined with network discovery and Windows penetration tests to reduce cost
- Some preparatory work
- Provide good benchmarks
- Provide excellent feedback on policy and standards



## Database and Internal Application Tests

- Databases and applications are the most vulnerable to internal attack
- Database tests can be partially automated
- Applications require manual testing (cannot be reliably automated)
- Need staff involvement during testing
- Annual tests are sufficient (unless the application changes)



## Wireless Penetration Tests

- Sensible scope can reduce cost significantly (AP audit vs endpoint audit vs penetration test)
- Wireless testing requires manual elements (cannot be automated)
- Need staff involvement during testing
- Annual tests are sufficient (unless the wireless network changes)



# Endpoint Penetration Tests

- Laptop tests can be straightforward if encryption correctly deployed
- Desktop tests can be relatively low-cost
- Smartphones and BlackBerrys are simple to test
- Must include tests of specialised servers (e.g. BlackBerry Enterprise Server)
- Annual tests are sufficient (unless the devices change)



# Social Engineering Tests

- Increasing requirement for these tests as criminals alter their methods
- Should include email (phishing), telephone and on-site tests
- Relatively low cost
- Excellent indicator of staff security awareness
- Are best deployed as part of staff awareness programme



# Threat and Vulnerability Analysis

To reduce costs we need to focus on high impact issues, so we need a methodology:

- Risk sources
  - Legal, regulatory, policy, audit, disaffected staff, criminals, vandalism ...
- Risk vectors and scope
  - Internal audit, attacks against Internet-facing hosts, internal attacks, on-site criminal attacks, telephone attacks, email attacks, data loss, endpoint thefts ...
- Vulnerability analysis
  - Known vulnerabilities, existing controls and mitigation, gap analysis, test results ...
- Impact analysis
  - Consequences of non-compliance, successful attacks, data loss, theft ...



# Partial Example Using CIA and 0-5 Rating

| Risk source           | Risk vector and scope           | Vulnerability analysis   | Impact analysis   |
|-----------------------|---------------------------------|--|---|
| Disaffected employees | 1. Windows privilege escalation | 1. Poor quality passwords<br>2. Systems not patched up to date<br>3. Inadequate logging and analysis | 1. Wholesale destruction of information (A5)<br>2. Wholesale corruption of information (I5)<br>3. Theft of sensitive information (C5)<br>4. Fraud (5) |
| Disaffected employees | 2. Remote access                | 1. Inadequate logging and analysis<br>2. Inadequate firewalling                                      | 1. Destruction of selected information (A3)<br>2. Corruption of selected information (I3)<br>3. Theft of selected information (C3)                    |



# How to Choose What to Do

## What to test?

- Threat analysis
  - What are the real threats with high impact?
- Legal, policy and audit requirements
  - What must we do to remain compliant?
- Incidents
  - What has happened that worries us?
- Budgets
  - How can we get the most from our budgets?

## What to fix?

- Vulnerability analysis
  - What are the real vulnerabilities with high impact?
- Legal, policy and audit requirements
  - What must we do to remain compliant?
- Incidents
  - What must we fix to prevent a recurrence?
- Budgets
  - What can we afford to fix?



# Any Questions?

Peter Wood

*Chief Executive Officer*

First • Base Technologies

[peterw@firstbase.co.uk](mailto:peterw@firstbase.co.uk)

<http://firstbase.co.uk>

<http://white-hats.co.uk>

<http://peterwood.com>



**FIRST • BASE**  
*technologies*