Cyber Resilience:
The Good, the Bad, the Ugly ... and the Retired

Peter Wood
Peter Wood

Race Driver, Musician, Partner at Naturally Cyber LLP

• Engineer, IT and security professional since 1969
• Founded First Base Technologies in 1989, the UK’s first cyber security firm
• Fellow of the BCS, Chartered IT Professional, CISSP, MCIIS
• Member of ISACA, Mensa
• Security evangelist
• Evo driver
• EDM musician
My short history of cyber security
1950s
1960s
1990s

COMPSEC '95 paper abstract
Security implications of network infrastructure migration

COMPSEC '96 paper abstract
Intranet security: Peter Wood, First Base

Compsec '97 paper abstract
NT server security, audit and control

Compsec '97 paper abstract
Internet E-mail security

Advanced Internet Security
A one-day Workshop

As the Internet's popularity continues to increase and many firms begin to implement Internet connections, security becomes a major issue. How real are the threats and how genuine are the counter-measures? How do firewalls help combat threats? What is the difference between one firewall and the next? Why is encryption important to me? What are digital signatures, authentication and certification?
What does the landscape look like today?
The enemy is sophisticated and strategic

What was advanced is now average

- Well planned, strategic approach
- Automation assisted manual attacks
- Social engineering, especially phishing
- Sophisticated malware
- Clear objectives
- Lots of resources
Apparently we are still ‘cyber novices’

Vast majority of countries are unprepared (%)

- Belgium: 74 Novices, 15 Intermediates, 10 Experts
- France: 81 Novices, 13 Intermediates, 6 Experts
- Germany: 19 Novices, 70 Intermediates, 11 Experts
- NL: 76 Novices, 15 Intermediates, 8 Experts
- Spain: 76 Novices, 15 Intermediates, 9 Experts
- UK: 72 Novices, 18 Intermediates, 10 Experts
- US: 73 Novices, 16 Intermediates, 11 Experts

https://www.hiscox.co.uk/cyberreadiness
This leads to weaknesses in defensive posture

- Poor understanding of cyber threats
- Staff ignorant of threats and impact
- Inadequate awareness programmes
- No formal threat and risk analysis
- No threat-led (red team) testing
- Missing policies and procedures
- Check-box thinking
And weaknesses in infrastructure

- Unpatched systems and applications
- Excessive access permissions
- Multiple copies of valuable data
- Sensitive information on endpoint devices
- Access for staff who have left the business
- Easy privilege escalation
- Inadequate remote access controls
- Excessive third-party access
What do we find when we test?
External vulnerabilities

- Two-factor authentication not enabled: 67.62%
- File upload facility: 32.79%
- Cross-site scripting: 22.54%
- Poor Citrix Configuration: 21.00%
- Excessive services available externally: 19.67%
- SQL injection: 16.80%
- Cross-site request forgery: 14.75%
- Plain text passwords in database: 3.28%
Internal vulnerabilities

- Weak passwords: 65.63%
- Missing patches: 56.25%
- Default credentials: 46.88%
- Default SNMP community strings: 43.75%
- Obsolete Windows OS: 25.00%
- HP System Management Vulnerabilities: 12.50%
- Insecure SMB service: 15.63%
Results of one spear phishing test

• 3,066 employees clicked on a link in a phishing email
• 2,398 users entered their username and password
• Most passwords were single words
• 72% were 10 characters or less

 Threat Assessment: Email phishing is the most prevalent cyber security threat to organisations. Passwords grant the attacker access to external services such as VPNs, OWA and Cloud Services

 Impact: Gaining access to these services can provide an attacker with full, undetected, authenticated access to your data
Single-factor authentication may not be your best choice!

- We cracked 48% of 9,569 passwords
- 98% were cracked within two hours
- The remaining 2% were cracked over a week

Some password statistics from another test

<table>
<thead>
<tr>
<th>Base Word</th>
<th>Number of Occurrences</th>
<th>Percentage of Cracked Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>1332</td>
<td>29.1%</td>
</tr>
<tr>
<td>{company name}</td>
<td>163</td>
<td>3.56%</td>
</tr>
<tr>
<td>monday</td>
<td>83</td>
<td>1.81%</td>
</tr>
<tr>
<td>passw</td>
<td>57</td>
<td>1.25%</td>
</tr>
<tr>
<td>{building name}</td>
<td>52</td>
<td>1.14%</td>
</tr>
<tr>
<td>tuesday</td>
<td>43</td>
<td>0.94%</td>
</tr>
<tr>
<td>friday</td>
<td>39</td>
<td>0.85%</td>
</tr>
<tr>
<td>scanner</td>
<td>32</td>
<td>0.7%</td>
</tr>
<tr>
<td>june</td>
<td>32</td>
<td>0.7%</td>
</tr>
</tbody>
</table>
We Need Cyber Resilience
We must be sophisticated and strategic
Accept that there is no silver bullet

Known • Predictable • Unknown • Unpredictable • Uncertain • Unexpected
Gartner says …

Take the money you’re spending on prevention and begin to drive it more equitably to detection and response. The truth is that you won’t be able to stop every threat and you need to get over it.

A dedicated, well-financed actor who is after something in your enterprise is going to get it, even if they use the weakest link, people, to do so.

This means adapting your security setup to focus on detection, response, and remediation. That’s where the cybersecurity fight is today.

In the future it will most likely move to prediction of what’s coming before anything happens.

Earl Perkins, research vice president, during the Gartner Security & Risk Management Summit 2017

The Information Security Forum view

Information security

Cyber security

Cyber resilience

Unknown, unpredictable, uncertain, unexpected

Known non-CIA

Known CIA
The Five Pillars of Cyber Resilience

Prepare / Identify → Protect → Detect → Respond → Recover
To successfully face and overcome an attack, you must thoroughly understand your organisation’s security and risk posture.

This means painstakingly identifying your vital information, conducting an assessment that includes all known security vulnerabilities, and establishing a baseline which you will compare with your peers.
The second pillar is about implementing safeguards to limit or contain the impact of an attack or breach.

Your goal is to protect your infrastructure and data from malicious attack and accidental exposure.

All three areas - people, processes, and technology - are important to your protection.
The Detect pillar focuses on developing activities to rapidly identify an attack or a breach, assess the systems that may be affected, and ensure a timely response.

To effectively minimise any damage, you must have the necessary detection and response policies, processes, and technologies in place.
The Respond pillar addresses activities that accelerate remediation and contain the impact of an attack once detected.

Whilst there are many solutions and services available to help, much of what is needed involves people and processes internal to your business.
Recover

This stage involves developing systems and plans to restore data and services after an attack.

Even if you respond quickly to a cyber breach, there may be consequences for people, processes and systems. An effective recovery depends on a clear and thorough recovery plan.
Getting started

1. Present to stakeholders and obtain buy-in
2. Form a Cyber Resilience group
3. Conduct a high-level gap analysis
4. Create a prioritised activity list
5. Produce a realistic roadmap
Don’t let this be you!

Management

Security
Peter Wood

https://naturallycyber.com