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

Peter Wood

N@turally Cyb3r

Helping companies develop cyber security instincts

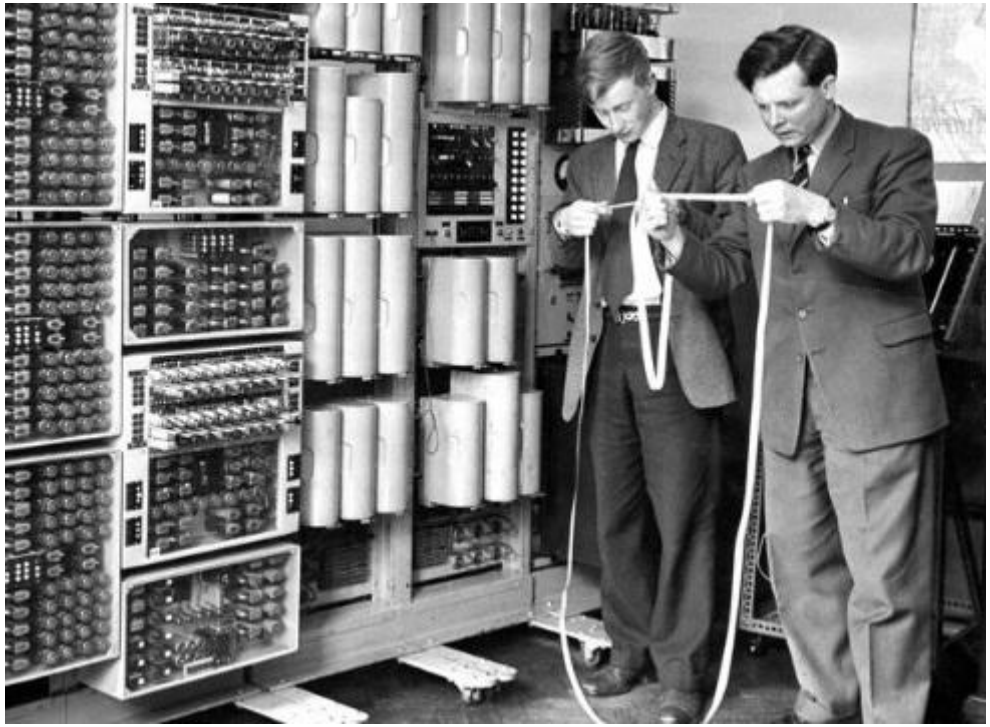
Peter Wood

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

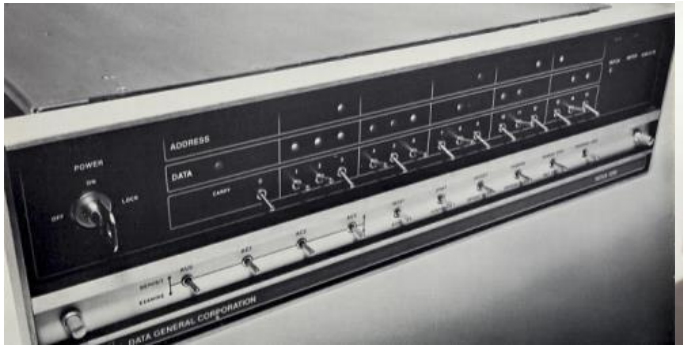
1950s



1960s

N@turally Cyb3r

1970s



1980s

1990s

COMPSEC '95 paper abstracts

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

BS 7799 IMPLEMENTATION SEMINAR

As the BS 7799 and c:cure scheme manager, we are able to ensure t

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?

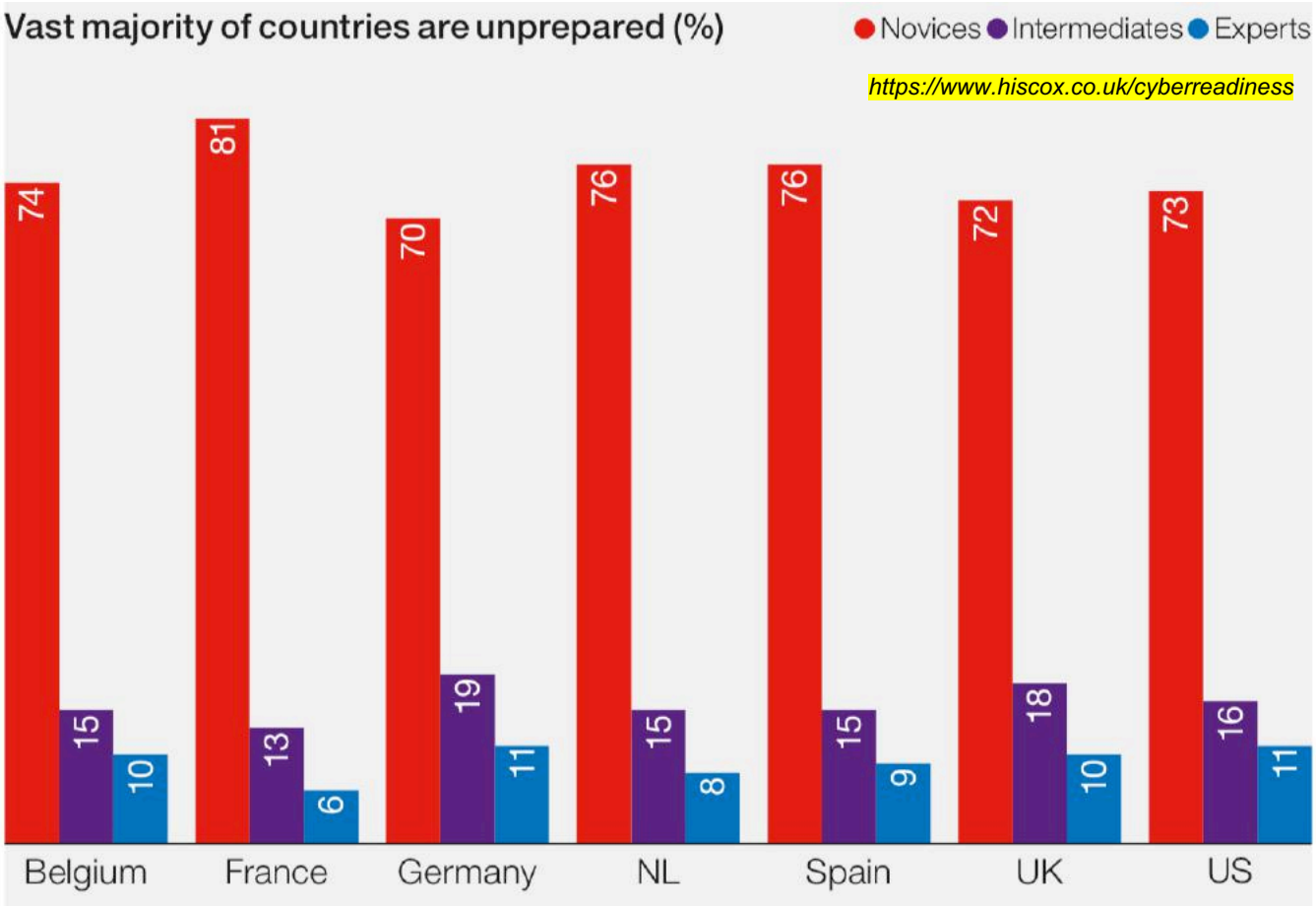
The enemy is sophisticated and strategic

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

Background Research	Social Engineering	Control Your PC	Explore the Network	Take Control	Find the Data	Steal the Data
• Internet searches • Social networks • Metadata • Phone calls • 192.com	• Spear phishing • USB attacks • Phone calls • Fake staff • Service staff • Visitors	• Malware • Key logging • Physical exploits • Wireless intercepts	• Servers • Desktops • Network devices • Firewalls • Wireless	• Windows admin • Network admin • Business apps • Database	• Strategy • Intellectual property • Marketing plans • HR data • Finance • Salaries	• VPN • Wireless • Email • FTP • Extranet • Physical devices

Apparently we are still ‘cyber novices’



This leads to weaknesses in defensive posture

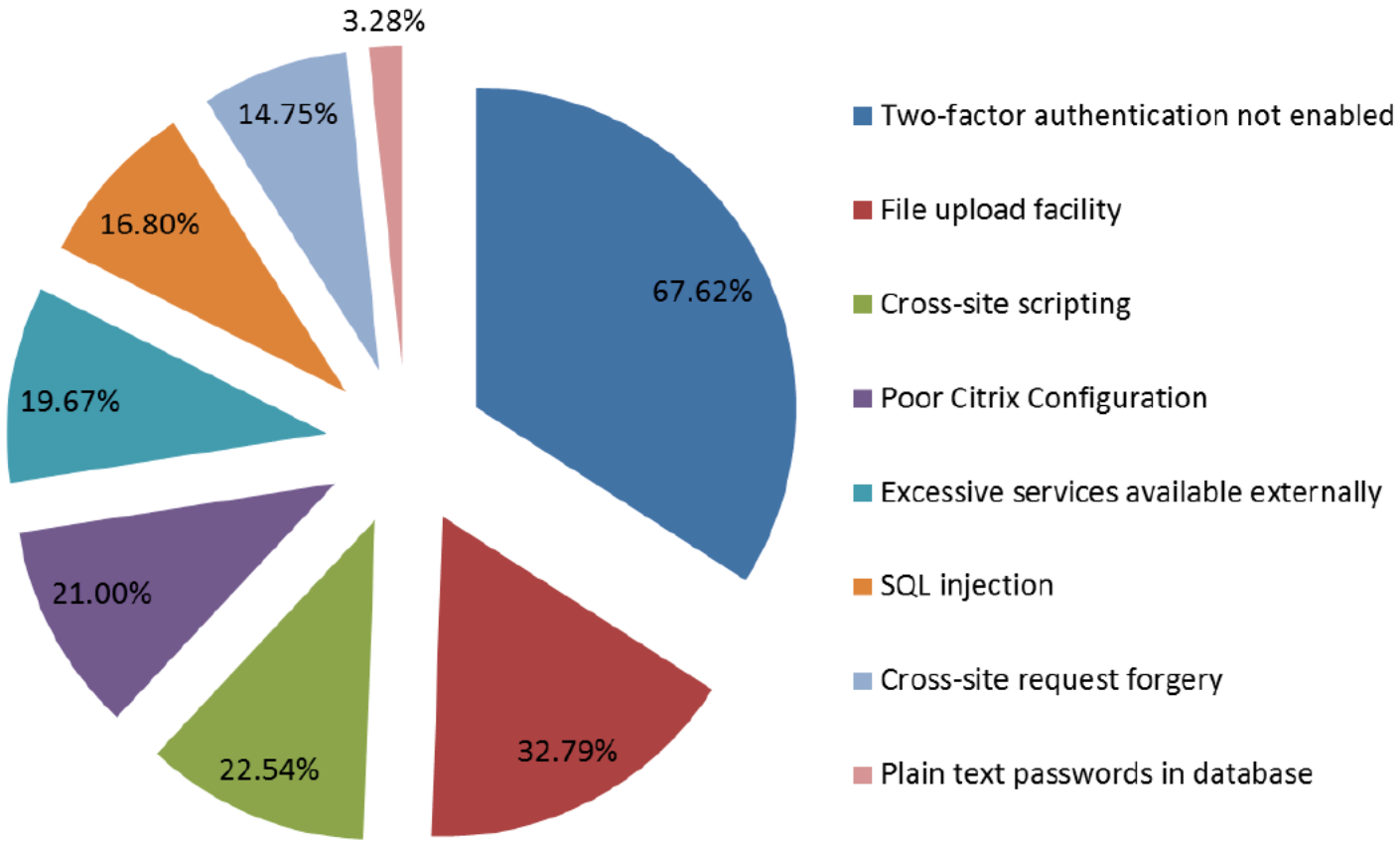
- Poor understanding of cyber threats
- Staff ignorant of threats and impact
- Inadequate awareness programmes
- No formal threat and risk analysis
- No threat-led (red team) testing
- Missing policies and procedures
- Check-box thinking

And weaknesses in infrastructure

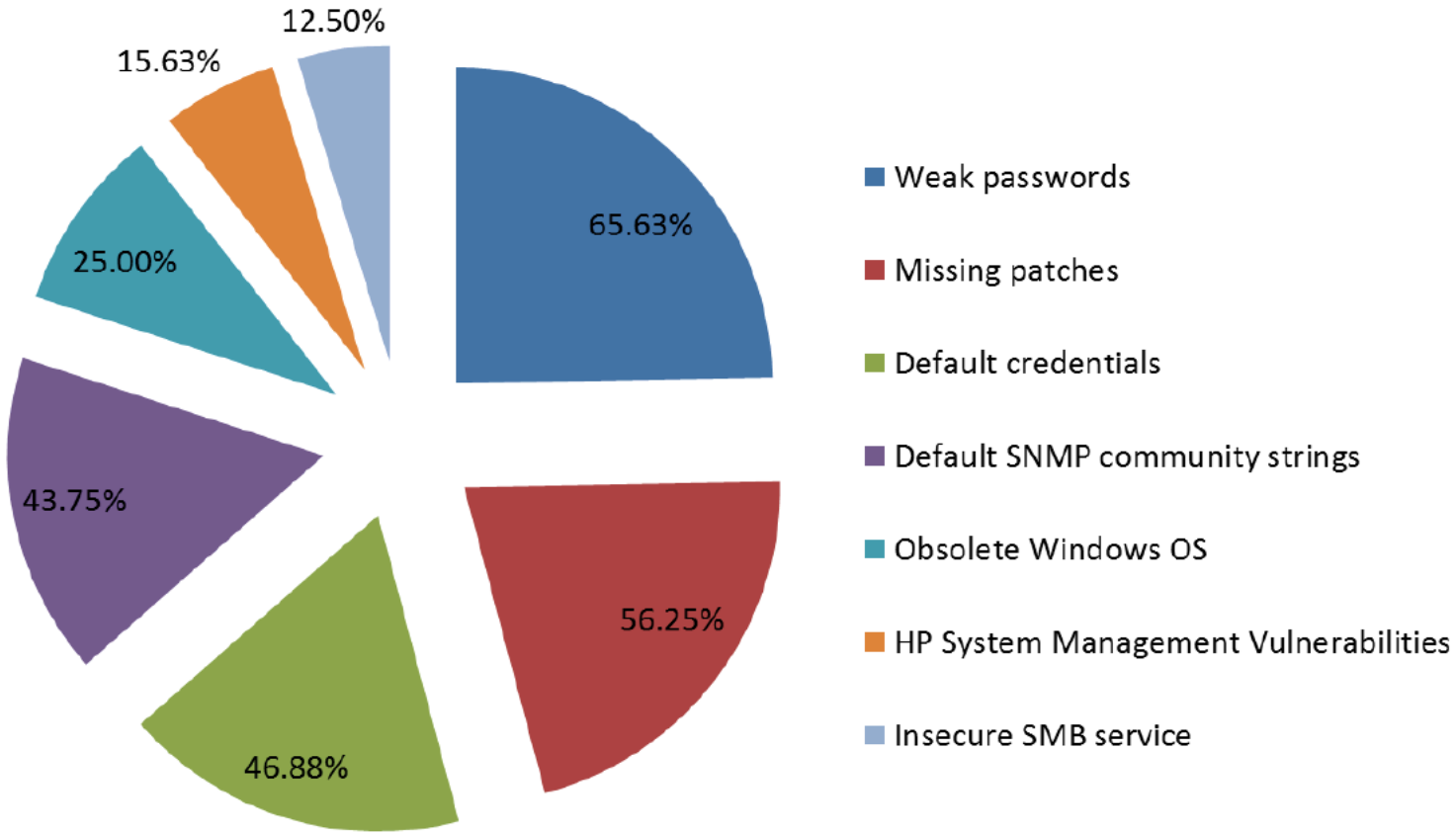
- Unpatched systems and applications
- Excessive access permissions
- Multiple copies of valuable data
- Sensitive information on endpoint devices
- Access for staff who have left the business
- Easy privilege escalation
- Inadequate remote access controls
- Excessive third-party access

What do we find when we test?

External vulnerabilities



Internal vulnerabilities



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

Some password statistics from another test

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

Base Word	Number of Occurrences	Percentage of Cracked Passwords
password	1332	29.1%
{company name}	163	3.56%
monday	83	1.81%
passw	57	1.25%
{building name}	52	1.14%
tuesday	43	0.94%
friday	39	0.85%
scanner	32	0.7%
june	32	0.7%

We Need Cyber Resilience

We must be sophisticated and strategic

Accept that there is no silver bullet

Known • Predictable • Unknown • Unpredictable • Uncertain • Unexpected

Background Research	Social Engineering	Control Your PC	Explore the Network	Take Control	Find the Data	Steal the Data
• Internet searches • Social networks • Metadata • Phone calls • 192.com	• Spear phishing • USB attacks • Phone calls • Fake staff • Service staff • Visitors	• Malware • Key logging • Physical exploits • Wireless intercepts	• Servers • Desktops • Network devices • Firewalls • Wireless	• Windows admin • Network admin • Business apps • Database	• Strategy • Intellectual property • Marketing plans • HR data • Finance • Salaries	• VPN • Wireless • Email • FTP • Extranet • Physical devices

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.

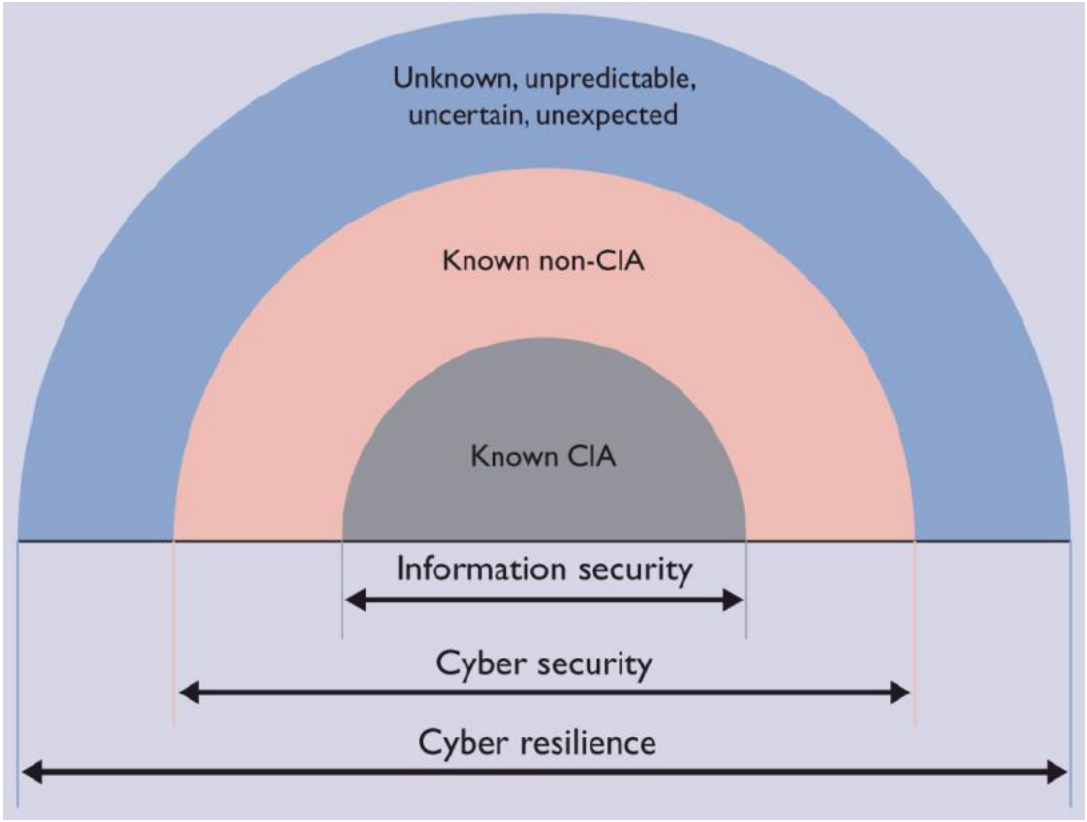
This means adapting your security setup to focus on detection, response, and remediation. That's where the cybersecurity fight is today.

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

https://www.gartner.com/smarterwithgartner/5-trends-in-cybersecurity-for-2017-and-2018/

The Information Security Forum view



ISF Cyber Security Strategies: Achieving cyber resilience, November 2011

The Five Pillars of Cyber Resilience

Prepare / Identify

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.

Protect

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.

Detect

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.

Respond

The Respond pillar addresses activities that accelerate remediation and contain the impact of an attack once detected.

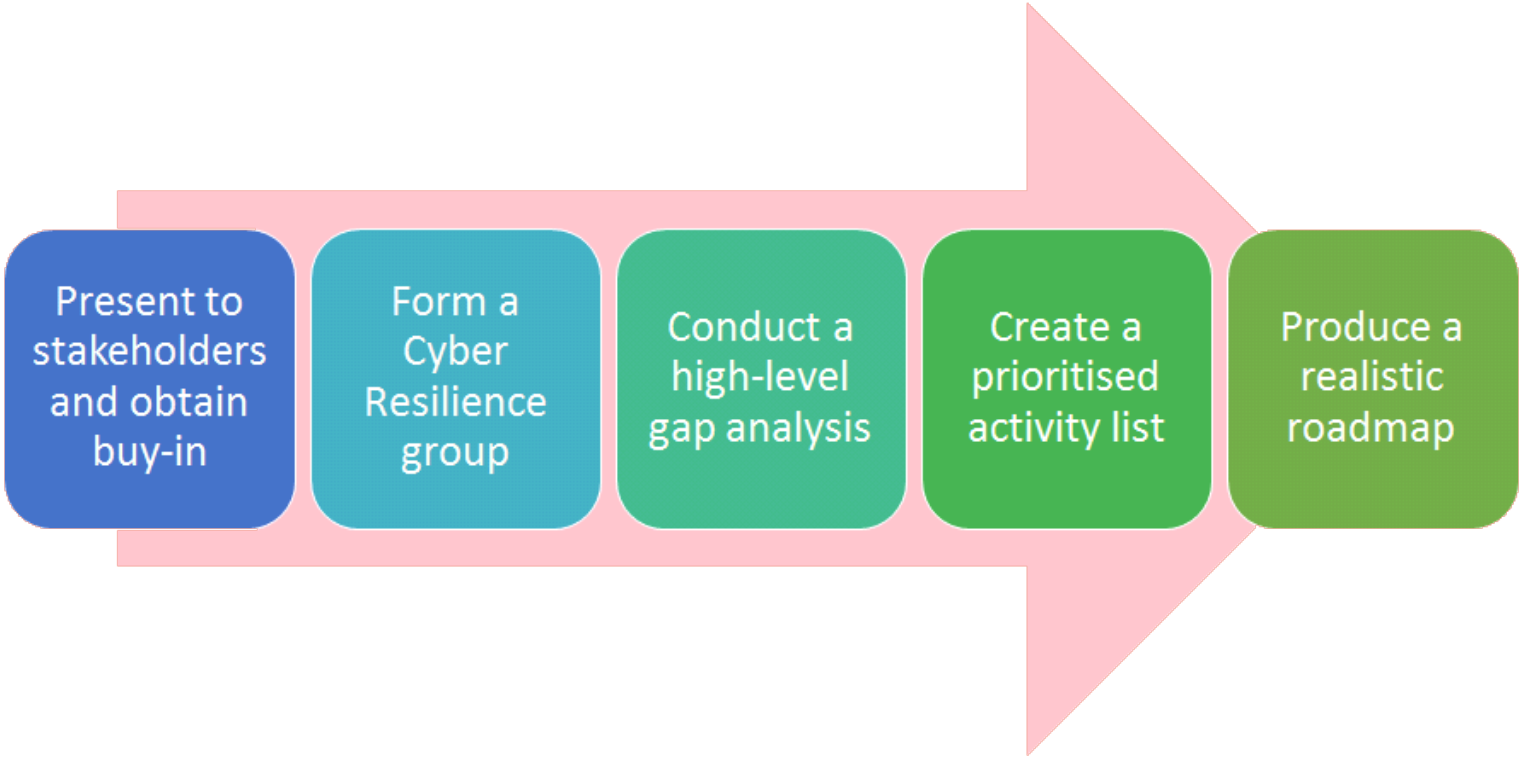
Whilst there are many solutions and services available to help, much of what is needed involves people and processes internal to your business.

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



Don’t let this be you!

Peter Wood

N@turally Cyb3r

Helping companies develop cyber security instincts

https://naturallycyber.com