HACKERS, SPIES, THIEVES AND STARTUPS

HOW TO PROTECT YOUR CROWN JEWELS, IN PLAIN ENGLISH.

IN COLLABORATION WITH

CPNI
Centre for the Protection of National Infrastructure

Quince
The Human Dimension of Security

National Cyber Security Centre

SPONSORED BY OSI

QUICK START GUIDE

Principles

- Your company is a target.
- Culture change is needed.
- Only Senior Leadership can drive change.
- Cyber, Physical and People are a system.

Real-world

- Make security a regular board agenda item.
- Being on top of security is essential to investors.
- Vet your people carefully.
- Train your people and test your readiness.
- Secure your physical space.
- Travel & JVs bring risks.

Cyber

- 2-factor authentication on everything.
- Cybersecurity Essentials PLUS. (here)
- Use VPNs for casual WiFi settings.
- Need-to-know access to data and digital assets.

RESOURCES

High-level

- CPNI's Secure Innovation campaign and the Passport to Good Security for execs sets out best practice and provides prompts for the actions you need to take. There is also an NCSC Board toolkit to help you get the buy-in you need. It would be best if you took action regarding cybersecurity.
- The Security Considerations Assessment (SCA) process covers physical, personnel, cyber and cross-cutting security measures.
- The Trusted Research campaign covers research collaborations in risky jurisdictions.

Travel. CPNI has created Secure business guidelines: How to operate securely with overseas parties.

People/Insider threat. Understanding the risks you face:

- Role-Based Security Risk Assessment
- How to obtain an Overseas Criminal Record Check
- Personnel Security Maturity Model
- Reducing Insider Risk
- Employment Screening

Who can help?

People: **Quince** helps organisations understand and manage insider risk. They do this by applying world-class expertise to help senior leaders and boards:
- understand the risk and its impact
- identify significant gaps in their defences, and
- design and build the right capabilities to fill those gaps
You can contact Paul Martin and Richard Mackintosh.

Physical: CPNI list of consultancies with physical security experts listed here.

Cyber: These four firms (Ascentor, Hexegic, Tranchulas, Infosum) have been used successfully by OSI portfolio companies, but there are many others certified to assess cybersecurity essentials plus here.

Training

Your people are the first line of defence. Help them stay secure at home as well as at work.
CPNI has developed a series of security awareness campaigns designed to provide organisations with a complete range of materials they need:

- Think Before You Link
- It's OK to say
- Mail Screening Matters
- Workplace Behaviours Campaign
- Employee vigilance campaign

Technical resources

- Secure design principles: Guides for the design of cyber-security systems.
- Logging Made Easy self-install tutorial details how to improve your records so you can understand and address breaches.
- Supply chain security guidance. Proposing a series of 12 principles designed to help you establish effective control and oversight of your supply chain.
- Incident management guidance. How to effectively detect, respond to and resolve cyber incidents.
- Active Cyber Defence (ACD). The ACD programme seeks to reduce the harm from commodity cyber-attacks by providing tools and services, free at the point of use, that protects against a range of cybersecurity threats.
- Cyber Essentials Certification is a simple but effective, Government-backed scheme that will help you protect your organisation, whatever its size, against a whole range of the most common cyber attacks.
- The NCSC's guidance on how organisations can protect themselves in cyberspace, including the 10 steps to cybersecurity.
- Physical Security guidelines from CPNI on how to find specialists.
- NCSC's Exercise in a Box. It is an online tool that helps organisations find out how resilient they are to cyber-attacks and practise their response safely.

Community resources

- The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to allow UK organisations to share cyberthreat information in a secure and confidential environment run by the NCSC.
- Keep up to date—the latest NCSC weekly threat reports.
- CNI Hub. NCSC assured Products and Services that support the Cyber Assessment Framework (CAF) principles. View the full list of Assured products and services.