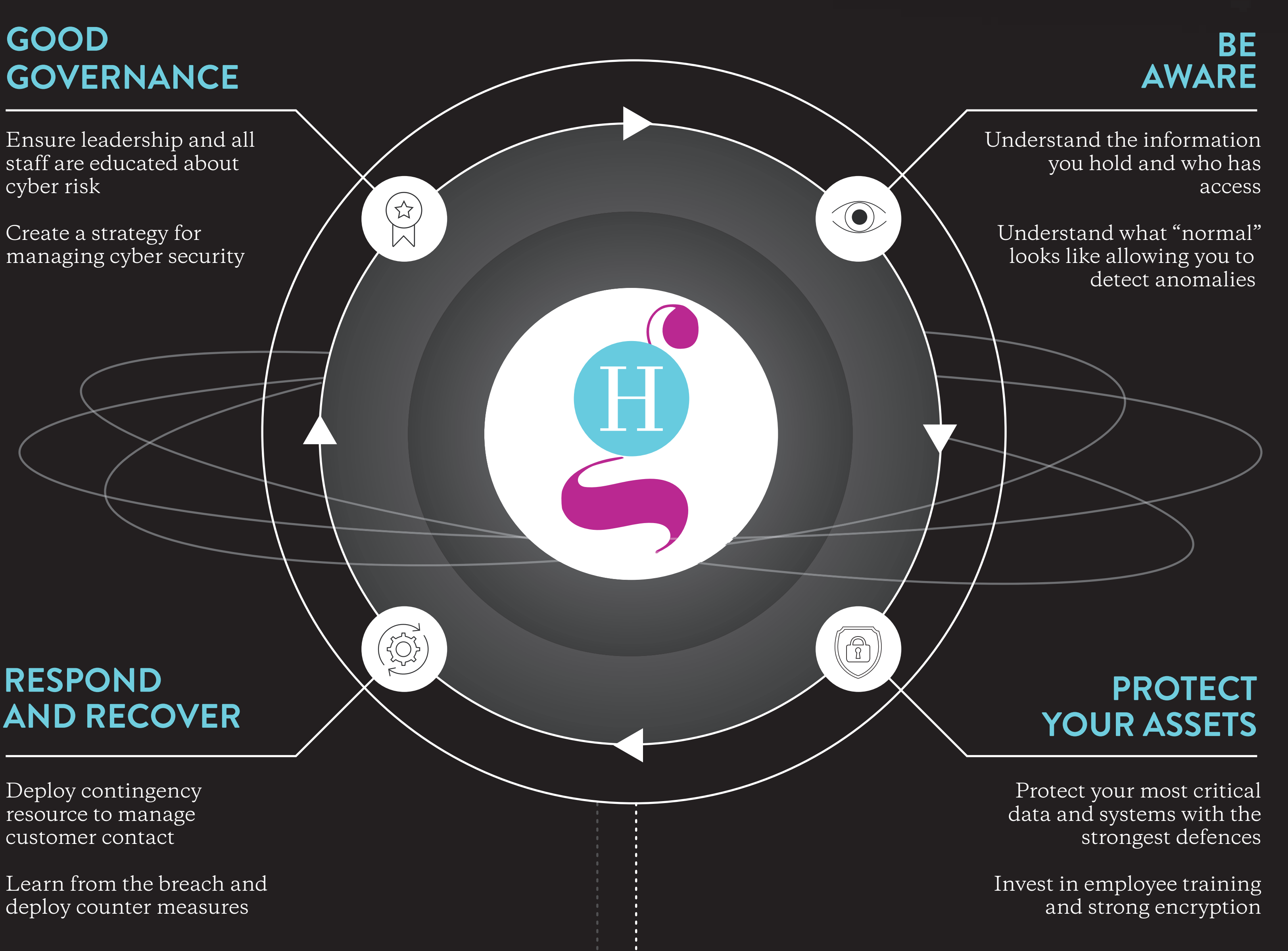
THE JOURNEY TO CYBER RESILIENCE

In March 2019, the FCA published a report on cyber resilience within financial services, based upon work conducted through the regulator's sector-specific 'cyber coordination groups' (CCGs). These groups aim to improve the cyber security practices within the sectors most crucial to the UK economy.

The FCA report provides firms with an outline of cyber resilience best practice, giving them an effective framework within which they can better defend against the increasing threat of cyber crime.

Working with cyber security specialists at Gadhia Consultants and taking onboard the guidance of both the FCA's CCGs and the National Institute of Standards and Technology (USA), we have outlined an ideal "journey to cyber resilience".

If your firm is looking to protect its assets, your customers and your reputation, there is no better time to start than right now, and no better place to start than right here.



GOOD GOVERNANCE

Ensure leadership and all staff are educated about cyber risk

Create a strategy for managing cyber security

BE AWARE

Understand the information you hold and who has access

Understand what "normal" looks like allowing you to detect anomalies

PROTECT YOUR ASSETS

Protect your most critical data and systems with the strongest defences

Invest in employee training and strong encryption

RESPOND AND RECOVER

Deploy contingency resource to manage customer contact

Learn from the breach and deploy counter measures

GOOD GOVERNANCE

- Use an "enterprise risk management" approach to share knowledge of cyber risk within your firm
- Ensure leadership is educated about cyber risk and that the Board puts plans in place to maintain operational and business resilience
- Present management information in a clear way

Gadhia Consultants are able to review, assure and even write cyber-security strategy. In-depth knowledge of regulatory structures and expectations will ensure your firm sets off on the right footing towards compliance.

BE AWARE

- Understand and audit the information assets that need to be protected
- Use "business impact analysis" to map out what business services need special protection, prioritised by how critical they are
- Map out what "normal" looks like in your day-to-day operations

YOU NEED TO:

1. Know who's who – tie users to accounts through "access management processes"
2. Identify users with privileged access
3. Monitor network and user behaviour
4. Collect the logs most relevant to your business
5. Apply strong access controls
6. Review and seek assurance that your log sources are working as intended

Understanding all potential risks and threats is paramount to defence. We know the landscape, and what could be lurking around the corner. We can be your guide.

PROTECT YOUR ASSETS

- Integrate cyber security policies, standards, procedures and controls into the change management process
- Layer protections so that the most critical data and systems are protected by the strongest defences
- Invest in employee training and strong encryption
- Perform penetration tests and 'war game' breach scenarios
- Seek independent assurance on your security arrangements

YOU NEED TO:

1. Test plausible scenarios
2. Make recovery decisions before incidents occur
3. Review information from previous incidents
4. Train staff on necessary skills or bring in specialist consultants to assist

Specialist consultants will be able to stress test your operations and even organise "war game" scenarios to test defences. Though you can't transfer responsibility for cyber security to a third party, trained resource can be deployed to bolster your cyber security operations.

DON'T TRANSFER RESPONSIBILITY FOR CYBER SECURITY TO A THIRD PARTY

GOOD GOVERNANCE

- To bounce back quickly from an attack, firms need to gather accurate data and deploy contingency resource to respond to customer contact and ensure business continuity
- Be prepared to be grilled by regulators – you need to be able to prove your firm had appropriate defences in place
- Learn from the breach by performing root cause analysis, then deploy counter-measures to prevent the issue occurring again

By bringing in expert security consultants, you will be able to quickly identify the weak links that led to the data breach and implement solutions that will prevent it happening again.

We can also help you prepare for post-event interviews with the regulator, providing you with the confidence and evidence needed for success.

Huntswood's resourcing capability can also rapidly deploy contingency resource to help you manage the influxes in customer contact that tend to follow a cyber security incident.

HUNTSWOOD