ASCOTBARCLAY™

www.ascotbarclay.com
info@ascotbarclay.com

SOLUTION HIGHLIGHTS.

7 STEPS TO HACKER HARDENED™

1. SECURITY LEADERSHIP & STRATEGY
2. FUSION SECURITY ADVERSARIAL MATURITY REVIEW
3. POLICY & GOVERNANCE
4. AWARENESS & TRAINING
5. SYSTEMS & ARCHITECTURE
6. MANAGED SECURITY SERVICES
7. AUDIT & LESSONS

PERPETUAL REVIEW PROCESS

HACKER HARDENED™ is a destination status. The journey is a get on anywhere, get off anywhere venture but eventually all blocks need to be well formed, well laid and the review process perpetual thereafter.

ABG assist our clients as efficiently as possible along this journey. We offer an end-to-end approach to helping mitigate the risk of a cyber security breach as well as managing the compliance risk associated with the impending GDPR regulations. Our service is available as a complete managed security service offering where we act as your Information and Cyber Security Team or transaction by transaction on individual elements. The choice is yours to suit your risk appetite and budget.

1 SECURITY LEADERSHIP & STRATEGY

Working with the main board and security sponsor to set strategy with a view to ensuring the organisation is Hacker Hardened®:

- Cyber security
- Compliance
- Legal
- Digital risk (including GDPR)

All appropriately assessed, resourced and mitigated.

Rotating your Chief Security Officer/Chief Information Security Officer (CISO) ensures oversight and shared perspective to yield the highest possible quality benchmark is attained and maintained. Many organisations don't need or have the budget to support a full time CISO or Data Protection Offer (DPO) – ABG offer experienced CISO/DPO resources as a more cost effective federated service on a part time basis to help manage, guide and develop internal staff to the point where they can either take over the role completely or more usually in part whilst keeping ABG on for oversight and escalation.

SMALL BUSINESS AWARDS 2016 CV MAGAZINE

winner Cyber Security Awards

2 FUSION SECURITY ADVERSARIAL MATURITY REVIEW

Red Team Testing of Security Vulnerabilities – We identify your areas of vulnerability before the 'bad guys' can exploit them. We then help you close the gaps to reduce your level of risk. Consultation with line management and technical (Penetration) review to gather:

- Physical
- Social
- Technical

Status and vulnerability assessment.

CORE DELIVERABLE: Security Adversarial Maturity REPORT with a recommended support model to mitigate where requested and required.

3 POLICY & GOVERNANCE

An organisation's Information Security Policy framework should be:

- **Accessible** – concise, to the point and clear it should not only be required reading but more importantly highly readable.
- **Realistic** – given the scale and complexity of the enterprise, its need to communicate with multi parties and that budgets are necessarily limited.
- **Encompassing** – covers all of the key attributes, outcomes and standards whilst also ensuring corporate compliance with the legislation in force and looming.

CORE DELIVERABLES: POLICY LIBRARY (Framework)

4 AWARENESS & TRAINING

HUMAN FACTORS represent the vanguard of known vulnerabilities across the majority of enterprises today. It is in this area that we find the weaknesses hackers are most likely to exploit. Core deliverables from our review typically include:

- **STAFF:** Two to Three hour staff interactive briefings on the need to take cyber security seriously and specifically the threats to your organisation
- **MANAGEMENT / EXECUTIVE:** One Hour executive briefings on Strategy into Execution, Business Impact of GDPR, the Cyber Threat Landscape and Executive Risk presented by Information Security in the enterprise.
- **ENTERPRISE:** Development of tailored Cyber Security training solutions for defined groups / teams and individuals (Strategic/ Operational/Technical). Please ask for detail on the specialist training we deliver for organisations and governments internationally.

ABG design and deliver Security Academies – Including specialist aspects such as Cellular Intercept, Intelligence, Insider Risk Management, Whale Phishing, Spear Phishing and more advanced areas such as Security Operation Centre Analyst Training and Specialist training in advanced security methodologies, tools and techniques.

5 SYSTEMS & ARCHITECTURE

Cyber Information, Data and Operational Technology Security

CORE DELIVERABLES (Typical):

- Hardening your technology architecture and critical systems
- Audit of Network and Application Security
- Advisory and implementation of Cyber Security Defensive technologies inc; Data Loss Prevention (DLP), Security Incident & Event Management (SIEM), Mobile Device Management (MDM), Certificate Management, Insider Risk Management, Real time Monitoring Solution(s)
- NET: **An independent, expert review and report on the IT security status of your organisation against the level of external and internal risk – Assistance to bridge identified gaps.**

6 MANAGED SECURITY SERVICES

750,000+
DATA SOURCES

ABG's Threat Monitor is a starter package for monitoring your organisation's threat surface whilst still benefiting from the full power of ABG's data collection partnerships and analysis experience.

We cover over 750,000 data sources from the deep and dark web, underground forums, to social media.

- Weekly customer threat surface reports
- Brand/Asset/Credential monitoring
- Vulnerability identification tailored to customer tech stack
- On demand analyst assistance to research IP's, domains, or suspicious attachments

Can be upgraded to a hosted 1 year subscription license for real-time Threat Monitor service that includes:

- 5 named user accounts for real-time Sec Ops access to the platform.
- Up to 6 real-time alerts relevant to the customer on the open, deep and dark web (IPs, IDNs, etc)
- Dashboard configured to customer's interests to detect emerging threats
- Expanded daily & weekly threat email reports

7 AUDIT & LESSONS

Helping the board stay fully informed, engaged and benefitting from Information Security

Adversarial and Compliance AUDITs. ABG pride ourselves that we know enough about the vagaries and uncertainties that characterize the world of Cyber/Data/Operational and Information Security never to allow complacency to colour our thinking.

- Revolving CISO – we rotate out CISO's regularly and often in an ad-hoc way to audit each other and to add additional perspective
- Senior CISO review – all of our clients will be oversighted by a member of our Senior CISO team
- Learned – evolution is a perpetual cycle – continuous improvement – recognition of an evolving and dynamic threat landscape.

Visionary – Our leadership is obsessive about understanding the security challenges faced by industry and our clients. We help to ensure that we stay at least a step ahead of our adversaries. Quarterly and annual review cycles ensure that forward momentum is maintained and a culture of security as a business enabler and market differentiator is realised. Taking past lessons and using them to secure future phases.

Helping ensure the board grasp the Information Security nettle, remove the sting then leverage your newly HACKER HARDENEDTM status as a valuable marketing differentiator

PERPETUAL REVIEW

The world isn't standing still and the continually expanding / evolving threat scape requires a cyclical and on-going oversight response.

Having achieved **HACKER HARDENED™** status ABG issue an annual certificate of authentication helping our clients stay in touch with and above the pre-set thresholds agreed and captured in the Information and data Security Policy and strategy that now acts as the internal 'bible' for standards.

ASCOTBARCLAY™

71-75 Shelton Street,
Covent Garden
London, UK, WC2H 9JQ

+44 (0)20 3897 2249
info@ascotbarclay.com
www.ascotbarclay.com