Board Governance of Cyber Risk

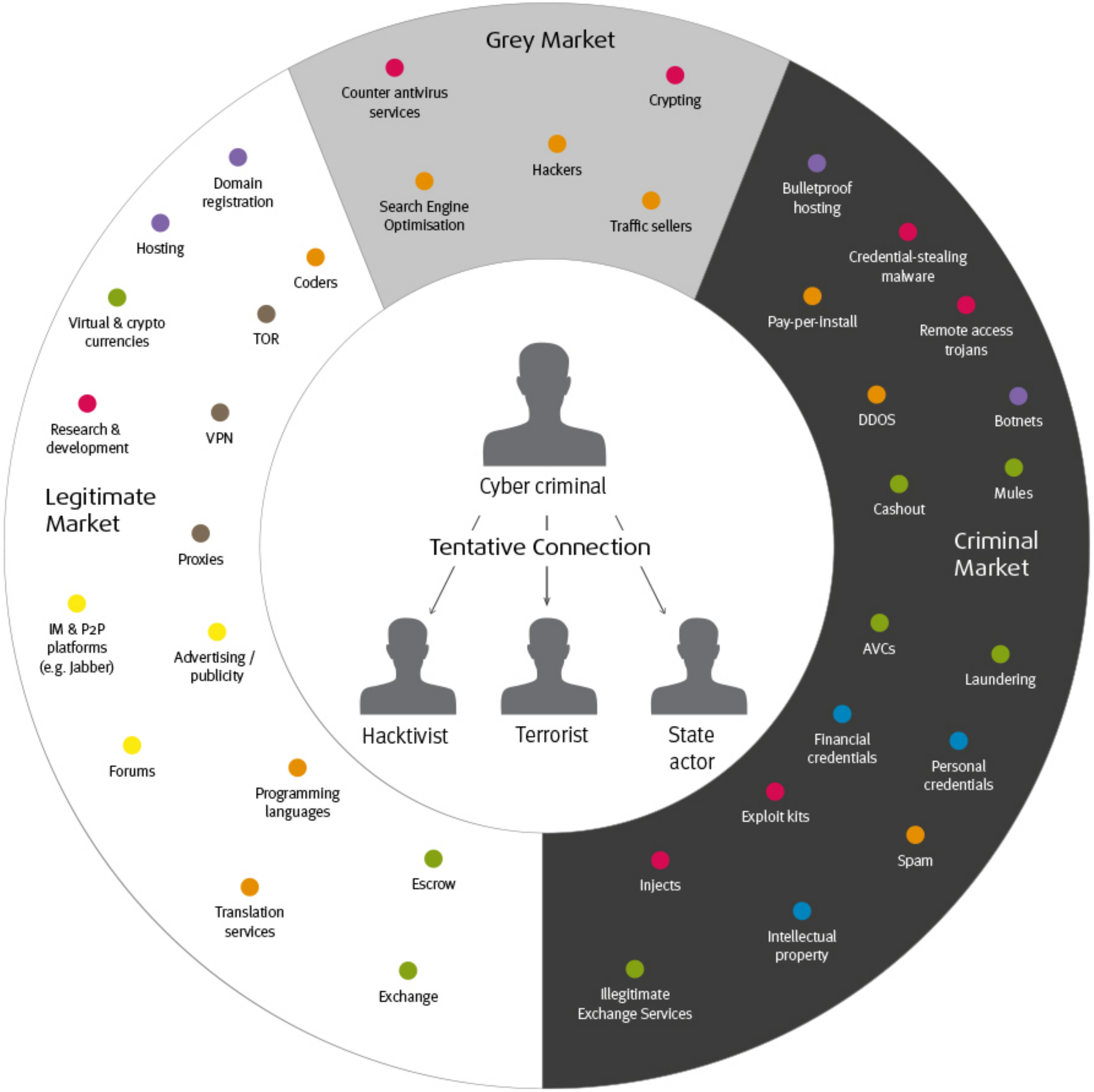
Stephen Page

Independent Non-Executive Director
and Senior Advisor to PwC

February 2017

sp@spmailbox.net
Oxford, UK
+44 1865 582444

Cyber threats are rapidly increasing in sophistication as organised criminals move into the digital age.



Source: National Crime Agency, *Strategic Assessment of Serious and Organised Crime 2015*

Role of the Board and Executive Management.

Board

Thoughtful, considered view of the threat and its impact on this business

Board* in its direction-setting role

- ⊙ Establish the risk appetite (including what will not be protected)
- Assess (and continually re-assess) the threat and its implications for strategy
- Help management to set values, beliefs, limits, ethical boundaries (eg inter-business sharing, employee/supplier monitoring, speed-vs-security)
- Help to solve “big” questions of structure, strategy, pace, disclosure, ethics…

Executive management

- ⊙ Deliver a mitigation programme to close any gaps—at the right pace
- Define policies and operate controls in line with board’s risk appetite
- Appoint senior leaders (not just IT) with accountability and influence
- Sustain insight and capacity (including in-house, third-party partnerships and industry peering) across IT, HR, Commercial, and throughout line business
- Develop an appropriate culture in line with board’s risk appetite

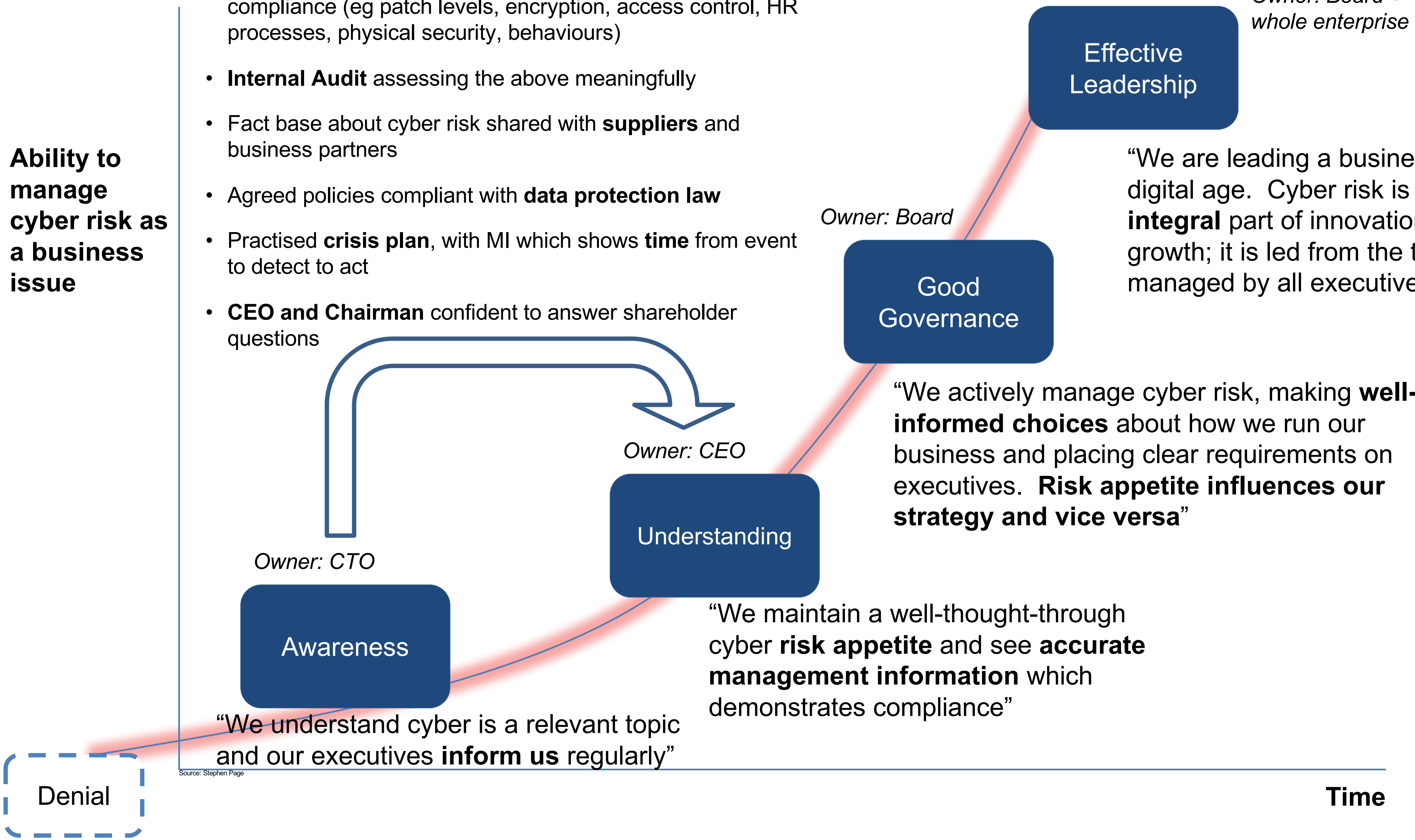
Board* in its assurance role

- ⊙ Inspect measurement system for focus on the right outcomes
- Assess strength and independence of assurance (“three lines of defence”)
- ⊙ Assess (and seek proof of) crisis readiness

* Board has these responsibilities, but detailed analysis is usually through a subcommittee eg Audit & Risk.
For companies with significant risk exposure, consider creating an Information Risk Committee of the Board.

Boards are developing stronger ownership, supported by MI and an intelligent dialogue about risk.

- **Risk appetite** based on board grip of **what data** we hold, why, for how long, and accessed by whom
- **Enterprise MI** which shows actual risk profile and compliance (eg patch levels, encryption, access control, HR processes, physical security, behaviours)
- **Internal Audit** assessing the above meaningfully
- Fact base about cyber risk shared with **suppliers** and business partners
- Agreed policies compliant with **data protection law**
- Practised **crisis plan**, with MI which shows **time** from event to detect to act
- **CEO and Chairman** confident to answer shareholder questions



Ability to manage cyber risk as a business issue

Time

Denial

Owner: CTO

Awareness

"We understand cyber is a relevant topic and our executives **inform us** regularly"

Owner: CEO

Understanding

"We maintain a well-thought-through cyber **risk appetite** and see **accurate management information** which demonstrates compliance"

Owner: Board

Good Governance

"We actively manage cyber risk, making **well-informed choices** about how we run our business and placing clear requirements on executives. **Risk appetite influences our strategy and vice versa**"

Owner: Board + whole enterprise

Effective Leadership

"We are leading a business in the digital age. Cyber risk is an **integral** part of innovation and growth; it is led from the top and managed by all executives."

Source: Stephen Page

A simple health check for use by NEDs.

Risk appetite and defence

Do we have the right skills?

- Strong knowledge of digital-age risks (and opportunities) around the board table
- Business leaders who instinctively think about data, how it is handled and protected
- Digital innovators who understand and value risk as much as speed
- CISO with sufficient competence, organisational/persuasion power, resources, independence, external network. Cyber also embedded in HR, commercial, …

Do we have the right fact base?

- Absolute clarity about what sensitive data the business holds, why, and for how long
- Clear view of where our risk exposure lies
- Clear understanding of what choices are being made for anything “new”
- Complete view of how data is shared with suppliers, partners and digital services
- Up-to-date view of legal and regulatory obligations for privacy and data protection

Are we making active, well-founded choices — from the top?

- Threat landscape | risk appetite | hard choices | management plan | delivery

Do we measure and improve?

- Enterprise MI which shows actual risk profile and compliance (e.g. patch levels, encryption, access control, HR processes, physical security, behaviours)
- A recognised framework against which we assess completeness of controls (eg ISO27001)
- “Three lines of defence” including independent review and capable Internal Audit

Breach response

Do we have a practised plan for breach response?

- A sound business understanding of data—to assess impact quickly
- Plans for both ‘big crisis’ and ‘slow burn’ issues which mature over a longer time frame
- Messages, media handling etc. aligned to a pre-agreed set of values
- Adequate technical capability to clarify ”what just happened” (e.g. thorough audit logs, pre-wired access for forensics) and capacity
- Preparation for the very big choices (eg under what circumstances do we pull the plug / shut the shop?)

Are we fast enough?

- Rapid response capability (including external help)
- Working the same hours as our adversaries
- Understanding what should be escalated - and doing so reliably
- Assessing business impact meaningfully

Are we willing to share incident intelligence with others?

- Law enforcement and intelligence community (eg Cyber Defence Alliance for banks)
- Peers within and beyond the industry
- Driving improvement in supply chain (and perhaps customers)
- ... vs our investor handling practices/values/regulators which may favour discretion