How COBIT 5 Can Help Reduce the Likelihood and Impact of the Top 5 Cyberthreats

By Sue Milton, CISA, CGEIT

COBIT Focus | 3 April 2017

2017 is here with cyberbreaches increasing, with their impacts rippling ever further into business and personal life. Are these threats too big to manage? Is cyberthreat management the ‘elephant in the room’?

Cyberresilience needs to be on the board agenda, but still too many boardrooms prefer to manage the risk with the Ostrich Control—hoping it will go away—exacerbated by the fact that security budgets continue to grow whilst answers to how much and what to target remain aloof.

The trick is to assess causes, how and where they manifest themselves, then define impacts and outcomes before choosing the appropriate controls. Simple in theory, a nightmare in practice because so much now is outside the direct control of our organisations. Originally, we talked about risk because of our ability to identify, assess and control them as they were mainly of internal origin. Those remain, and still need to be managed, but we also have a range of external issues over which we have no control in terms of origin, when, where, how, who. The game has changed from risk (internal) to threat (external) management.

It is difficult to address cyberthreats from the top because of the devil in the detail, often too many and varied for the leadership to appreciate the scale of the problem. Any hope of success requires a framework to keep us on track, hence COBIT® 5.

A new addition to the family is Transforming Cybersecurity, providing a high-level view of cyberthreat issues plus mappings to COBIT® 5 for Information Security. But as cyberthreats feed on traditional vulnerabilities, organisations still need a more comprehensive framework to ensure 360° coverage. COBIT® 5 for Risk, appendix B, provides a comprehensive set of practices covering both the technical and soft-skill aspects. COBIT® 5 for Assurance provides the means of identifying weaknesses. COBIT® 5 for Information Security identifies the controls needed to protect systems.

So we can:
- Find out where to look for vulnerabilities, human and technical (see COBIT® 5 for Assurance, sections B4-7)
- Understand why those vulnerabilities exist (see COBIT® 5 for Assurance, appendix D2; COBIT® 5 for Risk, appendix B, MEA01)
- Identify cause and effect to help understand the trade-offs that exist in all firms because resources are not limitless (COBIT® 5 for Risk, appendix B, AP008)
- Assess technical and behavioural security and control (COBIT® 5 for Information Security, appendices D-G)

My choice of threats come from Level 3 Communications as I believe they are representative of the attacks on the business community. If we apply COBIT 5 to them, (original source material from Level 3 Communications, embellished
by me using COBIT 5), we achieve this overview:

**Network and Application Layer Attacks**
**Causes**—DDoS tools readily available; unknown locations and number of disrupters with limitless patience; controls over hardware and software components not maintained
**Impacts**—Server and network disruptions; potential for a ‘piggy back’ attack to occur elsewhere
**Outcomes**—Business comes to a halt; opportunity cost of resolving the attack and rebuilding supply chain trust
**Controls**—Stopping an attack is very difficult to do so the firm must have robust internal detective, monitoring and corrective procedures, the ability to speak out on any suspicions and the agility to respond

**Social Engineering**
**Causes**—Genuine looking fake communication; vulnerable staff; weak governance, behavioural and security practices
**Impacts**—Critical information accessed; theft; physical and virtual access available to outsiders
**Outcomes**—Loss of competitive advantage; supply chain trust broken; overall reputation diminished; regulatory breaches; integrity of all other data now suspect
**Controls**—Many will be soft-skill controls such as antisocial engineering training at all levels and supportive management of staff; sound board/C-suite behaviour that complies with policies; speak up policies to allow anyone to say they may have been engineered. Technical controls are as above.

**Advanced Persistent Threats**
**Causes**—Exploiting vulnerabilities to create ‘backdoors’ to systems
**Impacts**—Credentials and data accessed and taken; as there is no obvious disruption, there is no obvious way of knowing how long it has been happening
**Outcomes**—As for Social Engineering
**Controls**—As for network application and layer attacks

**Organised Crime**
**Causes**—Ability to apply threats network application and layer attacks, social engineering, advanced persistent threats (APTs)
**Impacts**—As for network application and layer attacks, social engineering, APTs, but on a much larger scale. Victims are not only the organisation, but also the supply chain, customers and possibly their families and banks.
**Outcomes**—Intellectual property and sensitive data is now under the control of criminals for their benefit; more data available on the black market; ransom and blackmail demands
**Controls**—As for network application and layer attacks, social engineering, APTs; engaging with the police to ensure forensic evidence is preserved; engaging with lawyers to assess legal liability; establishing communications policy and practices for use with the media

**Major Data Breaches**
**Causes**—All the above
**Impacts**—Sensitive data exposed; business disruption
**Outcomes**—Loss of trust; high operational and reputational recovery costs
**Controls**—As for network application and layer attacks, social engineering, APTs and organised crime

**Conclusion**
If we want to focus on the cyberthreats:
• Start with *Transforming Cybersecurity* and apply the relevant aspects of *COBIT® 5 for Information Security*
• For a 360° assessment, assurance and action plan, broaden out to include *COBIT® 5 for Risk* and *COBIT® 5 for Assurance* as well
• The final cross-check is to see how the identification, control and management of the threats supports the overall goals of the organisation—the Enablers of COBIT 5 that enable an organisation to thrive—such as having a high-quality, customer-orientated service culture, increasing stakeholder value through enhanced effectiveness and efficiency.¹

By better controlling just one threat, the likelihood and impact of others are reduced too. Heads up please to see and deal
with the elephant in the room.

Editor’s Note
This article originally appeared as a blog post on the APMG International website. It has been reprinted here with permission.

Sue Milton, CISA, CGEIT
Is a professional IT auditor and governance specialist who has a profound understanding of the intangible aspects of governance, such as organisational behaviour, stakeholder relationships and the interaction between people and IT, that influence the effectiveness of working relationships within and between organisations. During 2015-16, Milton worked with the South African Development Community on managing the intangible risk to governance, with the Asian Development Bank to assist Myanmar’s transition to a market economy, and with APMG International to promote COBIT 5. She now concentrates on the governance challenges of the UK government’s green paper on proposed changes to the nation’s corporate governance code, and the strategic and operational challenges of Brexit, cyberthreats, and the EU General Data Protection Regulation. Milton is a former president of the ISACA London Chapter who also lectures and writes articles on governance and IT-related subjects for a range of organisations. She regularly provides business comment to the Institute of Directors’ Policy Unit and provides comment on cybersafety issues to the media.

Endnotes