Embracing complex systems thinking as the foundation for a new cyber security paradigm

By Michiel Jonker, Director: IT Advisory at Grant Thornton

17 June 2017

Introduction

Too often cyber security is considered to be exclusively the domain of IT and cyber security specialists. This is unfortunate, as we are progressing towards a future where an interdisciplinary approach will be crucial to deal with complex systems and their systemic fragilities and breakdowns, where cause and effect are not evident at all. As an IT Auditor and Futurist I am in a privileged position to approach problems from a different angle, i.e. not in isolation, but from a broader contextual perspective, the bigger picture, the macro patterns crystallising over a long period of time – and what they mean for the assurance industry.

The Internet, initially, was perceived by many as a social system, promoting openness and data sharing, not security. In other words, cyberspace was not 'built' for the purpose of securing data. Since then, privacy and cyber security advocates, and many other role players, offered resistance and influenced governments to enact cyber security and privacy legislations in many countries, including South Africa. Today, two (seemingly) irreconcilable paradigms – i.e. openness and security – need to be balanced, making expectations around the likelihood to prevent security incidents more and more of a problematic issue. Too many executives and Boards have unrealistic expectations about the prevention of cybercrime.

Furthermore, cyberspace is a complex system, with more than three billion people (with a free will) interacting with each other on a daily basis - over and above the billions of machines and devices facilitating these interactions. And believe it or not, political, economic and social conditions in the world, to name a few contextual factors, are part of the bigger cyber security picture.

How fragile are we?

In 2014 the CIA and NSA didn't anticipate a scenario in which Russian intelligence operatives could pass on orders and amass troops near Ukraine's border in the old fashioned way (i.e. by making use of the old courier system, instead of electronic communication). As a result they were not aware of Russia's plan to invade the Ukraine. By using traditional methods, Russia essentially had an anti-systemic response of disengagement from the specific technology (i.e. cyberspace). The question is – can your organisation still disengage from cyberspace? Most probably not. In our urge for efficiency and effectiveness (i.e. by automating all tasks and connecting everything to the Internet), we create fragile systems. A reduction in redundancy or alternative (even manual) options, creates fragility. And if your organisation is inevitably adjoined to the Internet, it is open to the dark forces of the Internet – and you will have to manage amidst the systemic chaos.

Flawed thinking - our downfall

The Captain of the Titanic, E.J. Smith, once said:

"But in all my experience, I have never been in any accident… of any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort."

We create our own Black Swans by being too optimistic and over-confident in our capabilities to achieve success. As Smith relied too much on the Titanic's design to resist (prevent) all

disasters imaginable, we also place too much confidence in our 'secure' designs to prevent security incidents. Just as Smith did, we architect cyber security on the basis of success – which is an inaccurate assumption. In the future we will have no other choice but to architect on the basis of failure – and to adopt methods to deal with failures. Cyber security challenges will increase and systemic breakdowns will occur. It is inevitable. Get used to it.

Why traditional risk management and best practice are not enough to deal with cyber risks

Prof David Snowden* makes a case with his Cynefin framework as to why best practice is not suitable for complex systems. Best practice is past practice, and suitable for simple systems. Simple systems are stable systems, with clear cause-and-effect relationships. In simple systems the right answer is self-evident and undisputed. Simple systems are areas where very little changes, such as problems with an order processing system. Adjacent to a simple system is a complicated system, which belongs to the domain of good practice (and the expert) and where there might be multiple right answers. Though there is a clear relationship between cause and effect, not everyone can see it. In his words, a complicated system is like a Ferrari – it is possible to disassemble it and to put it together again (with the help of an expert, of course).

* Snowden, D.J. & Boone, M.E. 2007. A Leader's Framework for Decision Making. Harvard Business Review, R0711C, 1-9

A complex system, however, is complex because the complexity is in the relationship and interaction of multiple components or sub systems. For example, once you have uprooted your garden or the rainforest, you cannot bring it back to its previous state, as things won't be the same again. This is the domain of emergence – where solutions cannot be imposed on the system. Solutions will emerge as you continue (as they do during a crisis). For example, just after 9/11, airplanes were grounded in the USA. Shortly after the crisis, an effort was made to plan for the next crisis – for a situation where airplanes may have to be grounded again. The conclusion of this futile exercise was that although a list of airfields can be made, with additional information about the size of airplanes, the number of planes every airfield can take etc., it is totally impossible to determine, in advance, which airplane can land where. The answer or solutions will emerge during the crisis.

Traditional risk management as well as best and good practices don't deal in an adequate way with Black Swans and unpredictability – i.e. as an organisation you do have control over simple and complicated systems. But you don't have control over a complex system – like cyberspace – as there are currently more than three billion people (i.e. components of the complex system) on the Internet. These cyberspace actors' actions are unpredictable. If the plans of companies, like Google and Facebook, succeed, we can expect even more cybercrime when eight or nine billion people are on the Internet in the future.

Systemic cybercrime

Why are we heading for systemic chaos? Our urge for efficiency and effectiveness create fragile systems PLUS the rapid introduction of automation PLUS increased numbers of the global populations coming online (3bn vs. 7/8bn people with a free will and whose actions cannot be predicted) PLUS an increase in integration of all systems, platforms and people PLUS an increase in religious, political (and geo-political conflict), economic and job polarisation worldwide, will lead to the proliferation of organised crime syndicates who want to exploit government and corporate systems. Exponential Internet growth will lead to massive security challenges.

In certain circumstances the best predictor of future behaviour is past behaviour. Up to now we couldn't prevent the massive number of (known) cyber security breaches. What makes us think that we will be able to prevent cyber incidents in the future, whilst operating in a

complex system? We have already noticed systemic breakdowns and uncontrollable situations. For example, ransomware-as-a-service console is now commercially available on the Internet – so a buyer of the console can attack whoever is next in a very long line of cyber victims.

What is the solution?
There are a few (not so conventional) options, but space only allows me to focus, briefly, on two.

First, we need to deal with our obsession with preventive controls and best practice in a complex system. Preventive controls couldn't prevent the known (and unknown) incidents in the past, and will be less likely to do so in the future. We will have to learn to manage amidst the systemic chaos. We need to architect, not on the basis of success (with maybe successful preventive controls), but we need to architect on the basis of failure. In other words, we should be in a position to detect breaches in a very short period of time – and correct them. The question to a CIO should not be: "Why didn't your controls prevent the incident?" But rather, "How quickly did you notice it (in 1 day or 100 days)? And what did you do about it?"

Put in audit jargon, in the future we won't have a choice but to spend more funding on detective and corrective controls. Ransomware has already proven to us that corrective controls are basically the only type of control that remains in the toolkit to rely on.

Secondly, 2013's remote hacking of a dam's operating system in the USA (only announced in 2016) by an Iranian terror group laid bare the potentially devastating consequences of having critical networks integrated online. The hacker gained unauthorised access to the dam's office data systems, but luckily didn't have the ability to control it because the sluice gate happened to be disconnected for maintenance.

While conventional wisdom tells us that prevention is far better than dealing with the effects of a cyberattack, it is now very clear that we might not have a choice but to rely more on detection and correction and, in **ultimate** cases (i.e. extremely and critical national infrastructure, like nuclear plants or dams), it might even be better not to allow certain high risk networks to be online at all. We have to accept a future in which we should carefully consider what we interface with what, where we have a bit more balance.

An anti-systemic response is an approach of disengagement from a system's rules which you cannot beat – for example, guerrilla warfare compared to a conventional army's tactics. Avoidance might be a suitable alternative, in extreme cases, in a world where overconfidence in preventive controls (sometimes to the extent of arrogance) has let us down. To believe that we can handle the forthcoming 'tsunami' will certainly be our downfall.

What does this all mean for the assurance industry?
From an assurance perspective we are interested to establish that for a given financial period, the systems responsible for generating the data (concluding with financial statements), were processing the data in a complete and accurate manner – and that the data was generated in an authorised manner. In the future, the assurance profession will have to focus more on the integrity of detective and corrective controls. For example, after a data loss, due to a security incident, the audit should focus on whether data recovery controls in place were reliable to recover to a verified state of data integrity again (i.e. complete, accurate and authorised data) – and that evidence of this is available and verifiable. If an entity couldn't restore its operational and financial systems (which has happened in the past), a qualified audit report might be on the cards. This would naturally be an unpleasant outcome, especially if investors or bankers are on a Board's case.

- ends – (1818 words)

Issued by Strat Comms Advisory Services on behalf of Grant Thornton South Africa
Trevor Neethling +27 (0)84 242 8668 / trevor@stratcomms.co.za
Lianne Osterberger +27 (0)83 27 27 313 / lianne@stratcomms.co.za

For more information contact

Michiel Jonker
Director: IT Advisory
Grant Thornton
T +27(0)10 590 7240 | M +27825709478
E michiel.jonker@za.gt.com

Vanessa Evans
National Senior Marketing, Communications & BD Manager
Grant Thornton Johannesburg
T +27(0)10 590 7200
E vanessa.evans@za.gt.com

Follow us on Twitter: www.twitter.com/grantthorntonza

About Grant Thornton South Africa
Grant Thornton South Africa is a member firm of Grant Thornton International Ltd (GTIL). Grant Thornton South Africa was founded in 1920. We are leaders in our chosen market, providing assurance, tax and specialist business advice to dynamic organisations – listed companies, large privately held businesses and private equity backed organisations.

We employ 1100 people in South Africa with 100 partners and directors. Grant Thornton has a national presence with offices in Bloemfontein, Cape Town, Durban, George, Johannesburg, Nelspruit, Polokwane, Port Elizabeth, Pretoria, Rustenburg and Somerset West. In Africa we operate across 24 member firms in Algeria, Botswana, Congo, Côte d'Ivoire, Egypt, Ethiopia, Gabon, Guinea, Kenya, Libya, Mauritius, Morocco, Mozambique, Namibia, Nigeria, Rwanda South Africa, Senegal, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe and are ideally positioned to facilitate clients' expansion plans in these countries.

About Grant Thornton International Ltd
Grant Thornton is one of the world's leading organisations of independent assurance, tax and advisory firms. These firms help dynamic organisations unlock their potential for growth by providing meaningful, forward looking advice. Proactive teams, led by approachable partners in these firms, use insights, experience and instinct to understand complex issues for privately owned, publicly listed and public sector clients and help them to find solutions.

More than 47,000 Grant Thornton people, across over 142 countries, are focused on making a difference to clients, colleagues and the communities in which we live and work.