MANAGING THE ESCALATING CYBER RISK

Roger Camrass
CIONET UK

Discussion Documents June 22

Managing the escalating cyber risk

This article was written by Roger Camrass, Director of Research for CIONET International, and is based on conversations during a virtual event on 14th June 2022 on how to manage the escalating cyber risk. The event was sponsored by Zscaler

The move to hybrid working and multi-cloud services has expanded cyber threat vectors dramatically. Recent developments around the globe such as war in the Ukraine have further exacerbated this situation. As a result, state actors and cyber-criminals have intensified their efforts to disrupt corporations and damage critical infrastructure. As attacks become more frequent, legacy approaches such as firewalls may fail to meet the current challenges. It is time to re-evaluate cyber defences.

A view from the sponsor

According to Christoph Heidler, head of transformation strategy at Zscaler, organisations need to introduce a new approach based on Zero Trust to protect themselves from a growing number of state actors and criminals.

Christoph made an interesting comparison between modern public telephone switching networks where anyone can connect to a chosen third party without encountering controls, and the earlier days of telephony where calls could only be made by operators who set up connections and often listened into calls. This guaranteed tight security over all person-to-person communications. The latter scenario mirrors what Zscaler is advancing with Zero-Trust as today's best practice.

Who are the bad actors?

State actors such as Russia, Iran, North Korea and China have always been in the attack front line. Being state funded they use the most sophisticated tools and innovate at rapid pace. Global uncertainties have fuelled higher levels of attack in recent months, especially from Russia and China. The situation can only get worse. Inflation and recession will encourage more criminal activity at home as well as abroad.

Meanwhile the cyber defence sector is learning fast. Companies such as Zscaler are building powerful capabilities such as Zero Trust platforms with careful attention to ID management. We can expect that Quantum Computing will be deployed by state actors within a few years, breaking every conceivable defence. Innovation is needed in both the supply and customer segments to stay ahead of such aggressors.

Do boards take this seriously enough?

Several delegates spoke about their experiences dealing with boards. The feeling was that cyber itself does not resonate well with non-technical peers, only the broader aspects of risk mitigation appear to be relevant for discussion. Some delegates spoke about the need to include IT and Cyber in the corporate risk register. This requires quantification of risk and detailed risk mitigation procedures. Not all organisations or sectors have achieved this today.

Budgets for cyber defences vary widely between sector, for example financial services spends up to 20% of IT budget on security.

Boards do recognise that the world has become extremely volatile, and that business resilience is a key imperative. Attacks will occur so organisations must be prepared to respond quickly to reduce their impact on operations. Ukraine and global supply chain disruption are damaging business confidence. Tighter governance measures are required, especially in defending against cyber-attack.

One delegate suggested that CISOs should train to become story tellers rather than technical analysts. Boards respond well to stories even though they may touch on technicalities.

How do changes in the IT landscape affect security?

Many examples were given of transformational changes taking place within IT itself that opens the door for higher attack levels:

- Move to multi-cloud environments expands attack surfaces and complicates traditional defence measures such as firewalls.
- Data lakes can simplify access to valuable corporate data compared to fragmented data assets locked away in legacy systems.
- Migration of applications from legacy (often inert to attacks) to cloud native applications implies multiple releases, each more vulnerable to attack.
- Growing 'shadow IT' amongst the businesses as people deploy Software as a Service (SaaS) in front and back offices as well as relying on spreadsheets and low code programming.

Many of these additional risk factors can be addressed by tighter governance. At the design stage, procedures such as DevSecOps can build security into new applications and reduce both design costs and chances of attack. The move by some organisations to integrated (or more centralised) governance of IT can also help reduce vulnerabilities by imposing standard frameworks. Government seemed to be well placed here through a combination of support from NCSC, GCHQ and frameworks that are being promoted by cabinet office.

What are the most practical measures to adopt?

All delegates accepted that attacks cannot be reduced to zero however strong defences may be. Organisations must seek to understand and quantify the risk of cyber attacks and take advice from regulators to stay within acceptable guidelines. One delegate stressed the need to build detailed inventories of IT assets such as software, hardware and data. By knowing what you have, risk mitigation becomes more of a science than an art.

Next steps for CISOs, CIOs and CTOs

Both Zscaler and delegates offered much practical advice on how to deal with cyber attacks and reduce business risk:

- Accept that attacks will happen and that appropriate procedures must be in place to reduce their impact. This includes people, process and cultural acceptance of risk.
- Build security into every aspect of the evolving IT landscape, from cloud migration to changing vendor relationships. DevSecOps is important in this respect.
- Adopt Zero Trust as your overall security platform with associated multi-authentication covering ID management.
- Ensure that your board is fully conversant with associated cyber risks and understands that they have the ultimate responsibility for this aspect of business management.

Roger Camrass
Lead researcher

A pioneer of today's Internet as an ARPA research fellow at MIT in the seventies, Roger has spent over forty five years helping corporations harness the power of new technologies such as cloud, mobile communications, e-commerce, voice recognition and satellite. He was a partner at EY responsible for e-commerce during the dot.com boom. He is a graduate of Cambridge University and MIT, and a visiting professor at the University of Surrey.

See **rogercamrass.com**