IT/Technology Risk

Contents

What is IT/Technology Risk?

Every Community Scheme has an IT/Technology threat or risk profile based upon; its business model, the extent of the use of IT/Technology, reliance on IT/Technology, the nature of the industry they operate in, the type and extent of the assets they control or manage, the nature of connectivity to their systems, their geography and the vulnerability of their IT and technology systems.

IT and Technology risk are, ironically, ultimately best managed by people.

A culture of awareness and discipline from ALL people is required to manage the risks emanating from technology use. You also need to clearly define what is expected of staff using IT systems to help the Community Scheme mitigate the massive increase in technology risk. On-going risk education and awareness training are essential, e.g. adhering to strict password controls, segregation of capabilities on banking systems, updating anti-virus and operating system security software, not opening unsolicited e-mails or attachments that result in phishing scams, being aware of ransomware, smishing and vishing threats, not acting on bogus e-mails or instructions, being aware of identity theft, verifying payment details thoroughly before making any payments, being aware of confidentiality requirements and the need to protect personal data, etc.

The role of the network, firewall, and security software in eliminating many other technology risks (e.g. data theft, hacking, ransomware, and eCommerce fraud) is a basic requirement for managing these risks.

Given the integral role that technology and IT plays in every sphere of a Community Scheme's operations, this key area demands good governance – processes and procedures, policies, disciplines, controls, and risk mitigation, particularly in the areas of cybercrime, business continuity, and disaster recovery.

Technology and IT are complex and evolving environments, and risk controls have to be ongoing too. The roles technology and IT play, and their dependency varies for each Community Scheme, irrespective of size. The reliance on technology and IT needs to be assessed by each Community Scheme to assess and quantify the impact of a potential failure or loss

arising from these areas. In situations where the IT systems and networks are extensive and complicated, dedicated IT support services may be required, beyond just the use of outsourced ad-hoc IT support services. A dedicated IT information or security officer may well be required in large Community Schemes.

Technology also brings with it the risk of obsolescence. There will always need to be a trade-off between progress in technology and affordability of the latest technology by the Community Scheme. The back-up and support of technology systems, guarantees and warranties provided are very important considerations in the selection of both technology and associated service providers.

The Level of Controls and Security

The level of controls and security required will be dictated by several factors for example:

- The volume, sensitivity, importance, and "value" of the Community Scheme's data.
- The complexity and nature of the Community Scheme's operational environment.
- The extent of proprietary software and legacy systems being used by the Community Scheme e.g. systems for bookkeeping, billing, reservations, sales, mailing applications, accounting, and payments.
- Use of banking payment platforms.
- The extent of mission-critical systems e.g. access control systems and databases.
- Potential threats to the Community Scheme and its assets, e.g. cash balances, consumable stock holdings, payments profile, and size of payroll.
- The physical environment.
- The number of users of the IT and supporting systems.
- The extent of access to the systems (internet/apps/e-mail/log-ins/devices and network connections/remote access).
- The extent of home/remote office connectivity.
- Regulatory and compliance requirements.

Cybercrime

The growing threat and risks of cybercrime and security breaches are set to change the face of business operations going forward. Cybercrime is generally defined as any form of criminal activity involving the use of computers and the Internet. This can arise from both external and internal sources. Attacks can also be malicious and a form of sabotage. As technology and risk evolve, this will necessitate a forward-looking, and layered security response to protect your Community Scheme from new and as yet inconceivable threats. Cybercrime poses such a significant risk to larger Community Scheme's operations that it is now recommended as a critical reportable board agenda item.

One of the biggest threats facing any Community Scheme is the loss of data and systems. A balance has to be achieved between the availability and security of data within a Community Scheme. The integrity of data and the maintenance of information confidentiality is also of paramount importance from both a regulatory (Protection of Personal Information – POPI) and operational perspective.