The Information Security Forum (ISF), trusted resource for executives and board members on cyber security and risk management, today announced the release of *Blockchain and Security: Safety in Numbers*.

The organization’s latest briefing paper helps those involved in blockchain deployment to understand the main components of a blockchain network, identify security issues associated with developing or using blockchain applications, address security issues in a structured manner by determining security requirements, apply a secure systems development lifecycle (SDLC) and support live blockchain applications.

Often described in terms of anonymity and security, Blockchain is advertised as a game-changer for businesses, governments and criminals alike. However, as organizations rush to deploy applications based on blockchain technology, do the potential benefits outweigh the information risks? While the more familiar manifestations of blockchain – such as cryptocurrencies – are based on public (permission-less) blockchains, private (permissioned) or federated blockchains are increasingly of interest to organizations. Understanding the potential security issues, and how they can be addressed, is vital for any organization planning to use applications based on blockchain technology, especially considering a number of well-known blockchain breaches within financial services.

“Blockchain’s indelible and visible record provides many advantages. However, this record does not render blockchain immune from security issues,” said Steve Durbin, Managing Director, ISF. “Many of the security issues associated with developing and operating any application – such as managing an implementation, providing acceptable technical support and training staff – are still applicable to blockchain. The main security issues specific to blockchain relate to breaches of the integrity of the ledger and individuals performing malicious or fraudulent transactions.”
Blockchain introduces a relatively new concept based on trust in a distributed network of participants, some of whom may not be known. Blockchain risks are particularly acute considering that its security is built on assumptions that the:

- content of the blockchain ledger is both immutable and irrefutable
- underlying cryptography is secure enough to last the life of a blockchain application
- consensus algorithms are robust.

As blockchain is put to different uses, it is vital to look beyond the hype and understand its merits and disadvantages. After all, it may not always be the best solution to a problem; directories, databases and other types of data store still have value.

“While there may be a commercial advantage from being at the forefront of adopting blockchain, prudent organizations should be aware that blockchain is immature and unforeseen security issues may emerge,” continued Durbin. “Consequently, organizations should place a particularly strong emphasis on evaluating the risks of developing or using blockchain applications before trusting this innovative approach.”

The ISF provides guidance to organisations on how to work effectively with Blockchain, as well as covering all other areas of cyber security and risk management. This research is complements a comprehensive suite practical information security tools. Blockchain and Security: Safety in numbers is available now to ISF Member companies via the ISF website.