



A HOLISTIC APPROACH TO RISK MANAGEMENT

Stéphane Hurtaud, chief security officer of Belgo-French banking group Dexia, explains the four keys pillars of the company's approach to information security

July 2010

CASE STUDY

With the current wave of technologies enterprises are embracing – cloud, social media, and numerous others – it is essential to go back to basics, says Stéphane Hurtaud, chief security officer at Belgo-French banking group Dexia.

“One of the major pitfalls in information security is to see technology as the main driver in the identification of risk,” he says. “The reality is that we engage with new technologies on a daily basis, and each of them involves a new threat or risk.” Rather than addressing a specific threat, Hurtaud argues that organisations need to build their information security around a more holistic model.

Dexia is putting in place four main pillars designed to support this rounded approach to security:

Risk framework The framework must support robust risk management and identify the threats associated with introducing new technology. “Before starting a new virtualisation project at Dexia, we undertake an analysis to identify the different risk factors and gauge what needs to be done in terms of security controls from both a technical and engagement point of view,” says Hurtaud. This approach is key in justifying the need for IT security investment. “The board will ask what the balance is between the risk and the cost of mitigating against it.”

Asset awareness One of the fundamental challenges for information security is to identify the organisation's most sensitive and valuable data and applications. It is vital the security budget is targeted on those assets, he says. “It may seem like common sense to classify data by its importance but there are many organisations where that is at a very immature

level.” Hurtaud adds that classification needs to be application- rather than technology-centric. “IT asset classification should be based on identifying your critical business applications while also considering all the different assets that support those applications.”

Mutually supportive security “It is important to develop security in depth,” says Hurtaud. “You need multiple layers of defence throughout the IT system rather than to rely on any single control. Such mutually supportive controls – an application firewall, a network firewall, strict administrator access controls, and so on – ensure that if one fails, other controls mitigate against the risk.”

360-degree governance Organisations need to have sound IT security governance that relies on a well-defined security organisation reporting directly to a C-level executive, an isolated security budget and some well-defined IT security processes. This governance also has to cover all external partners, including outsourcing arrangements. “By outsourcing a discrete IT activity you transfer the risk to someone else but you are still the one who's responsible for that risk. So you have to develop specific controls to be able to supervise your contractors and have the assurance that the activity you are outsourcing is secure.

With such fundamentals in place, says Hurtaud, the risk associated with the introduction of new technologies becomes much more quantifiable and manageable. ●

● Stéphane Hurtaud is chief security officer at Dexia Group, the Brussels-headquartered bank with an operational footprint that spans Belgium, France, Luxembourg and Turkey.