LEGAL IMPLICATIONS OF INFORMATION SECURITY GOVERNANCE

by

VERINE ETSEBETH

submitted in partial fulfilment of the requirements for the degree

MASTERS OF LAW

in

CRIMINAL LAW

in the

FACULTY OF LAW

at the

RAND AFRIKAANS UNIVERSITY

SUPERVISORS: PROF MM WATNEY

PROF SH VON SOLMS

DECEMBER 2003

ACKNOWLEDGEMENT

- I wish to express my most sincere gratitude to my supervisors, professor MM Watney and professor SH von Solms, for their invaluable knowledge and guidance in the writing of this dissertation.
- On a personal note I would like to thank my mother for her love, support and patience. Thank you for always believing in me.
- Furthermore, I would like to thank a friend without whose help, support and patience this dissertation would never have become a reality. Your tireless efforts at helping me reach for my dreams go beyond friendship. I will never attain your level of excellence, but I'll look better while trying. Thanks S.
- Most importantly, I would like to thank my Creator.

"Life is no straight and easy corridor along
which we travel free and unhampered,
but a maze of passages,
through which we seek to find our way,
lost and confused, now and again
checked in a blind alley.

But always, if we have faith,
God will open a door for us,
not perhaps one that we ourselves
would ever have thought of,
but one that will ultimately
prove good for us."
- A.J.Cronin

ABSTRACT

This study conducts an analysis of the legal implications of information security governance, by defining information security governance, identifying those entities who should be concerned with this discipline, namely the board of directors and top management, assessing why the need for this discipline exists, and highlighting the benefits that will be derived from the effective implementation of this discipline. However, the focal point of this study centers around arguably the most important legal implication of information security governance, namely legal liability for non-compliance with information security governance. Particular attention is given in this regard to the fulfillment of the duty of care and skill/due diligence, which requires of directors, specifically within the information security domain, to take reasonable steps to secure the organisation's information assets. The conclusion is reached that in order for a director to fulfill his duty of care and skill/due diligence, and ultimately escape liability for failed information security, it is required of a him to educate himself on, be involved in, and be committed to the discipline information security governance in its entirety.

OPSOMMING

Hierdie studie onderneem ‘n analise van die regsimplikasies van inligtingsekuriteitsbestuur, deur inligtingsekuriteitsbestuur te definieer, die entiteite wat hulself moet bemoei met hierdie dissipline, naamlik direkteure en top bestuur, te identifiseer, ondersoek in te stel na die bestaansrede vir hierdie dissipline, en die voodele verbonde aan hierdie dissipline uit te wys. Die kruks van die studie is egter gesentreer rondom argumentsonthalwe, die belangrikste regsimplikasie van inligtingsekuriteitsbestuur, naamlik regsaanspreeklikheid vir nie-nakoming van inligtingsekuriteitsbestuur. In hierdie opsig word veral aandag geskenk aan nakoming van die plig tot sorg en vaardigiheid, wat van direkteure vereis, spesifiek binne die inligtingsekuriteitssfeer, om redelike stappe te neem om die organisasie se inligtingsbates te beskerm. Daar word tot die gevolgtrekking gekom dat, vir ‘n direkteur om aan sy plig tot sorg en vaardigheid te voldoen, en uiteindelik aanspreekilkheid vir mislukte inligtingsekuriteit te ontkom, daar van die hom verwag word om homself te onderrig in, betrokke te wees by, en toegewyd te wees aan die dissipline inligtinsekuriteitsbestuur in sy geheel.