BOTLHOLE LAW GROUP

IN ASSOCIATION WITH
NEILL ARMSTRONG
ATTORNEYS, NOTARIES & CONVEYANCERS
CORPORATE | CONSULTANCY | LITIGATION | TAX

JANUARY 2023

BULLETIN

ENTERPRISE RISKS OF BUSINESS EMAIL COMPROMISE

According to a report by Federal Bureau of Investigation (FBI)'s IC3 (Internet Crime Complaint Center):

- Between July 2019 and December 2021, BEC/EAC attacks surged by 65%;
- BEC attacks cost organizations approximately $43.3 billion between 2016 and 2021:
- BEC attacks cost organisations more than ransomware attacks.

Reflections on the case of *Hawarden v Edward Nathan Sonnenbergs Inc*

Here is what you need to know

The world of data and technology is fast paced, disruptive and complex, and so is the risk of threats that they present to enterprises. These risk threats have significant implications for risk management, they require complex strategies and methodologies to ensure that an enterprise is protected. Our advice to Clients is that the best approach to risk management is a proactive approach.In this Bulletin, we discuss the enterprise risks posed by use of email and shown in the recent court case of *Hawarden v Edward Nathan Sonnenbergs Inc*.

Nature of the claim

A delictual claim for pure economic loss caused by omission.

Brief factual background

The plaintiff purchased an immovable property from a third party seller who appointed the defendant, ENS attorneys, as the conveyancer in the sale transaction. The plaintiff paid the deposit required under the sale agreement and thereafter chose to pay the balance of the purchase price of R5.5 million by way of electronic transfer of funds directly into the defendant's trust account for the benefit of the seller pending registration of transfer.

The plaintiff made an electronic payment of the amount of R5.5 million into what she believed was the ENS account. The details of the ENS account had been emailed to her by a conveyancing secretary employed by the defendant. The ENS account details were specified in a pdf document attached to an email. Unbeknown to the plaintiff, her email account was hacked and the email containing the ENS account details was intercepted by an unknown fraudster and altered to reflect the fraudster's bank account details, resulting in the funds electronically transferred by the plaintiff being deposited in the fraudster's bank account as opposed to the ENS account. Upon discovery of the cybercrime, the plaintiff sued the defendant for the R5.5 million lost by the plaintiff as a result of the cybercrime.

The court's decision

It was held that:

- a duty of care exists between a purchaser in a conveyancing transaction and the conveyancing attorneys handling the transaction to prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking and spoofing of emails or of the fact that pdf attachments to emails containing sensitive information such as bank account details are not invulnerable to BEC.
- as an experienced conveyancer, the defendant understood the risks inherent in conveyancing transactions by virtue of its own prior knowledge of the dangers of BEC. The risk of BEC was thus foreseeable and the defendant was under a duty to guard against the harm eventuating. Its omission to do so was negligent in the circumstances.
- a duty of care exists between a purchaser in a conveyancing transaction and the conveyancing attorneys handling the transaction to prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking and spoofing of emails or of the fact that pdf attachments to emails containing sensitive information such as bank account details are not invulnerable to BEC.
- as an experienced conveyancer, the defendant understood the risks inherent in conveyancing transactions by virtue of its own prior knowledge of the dangers of BEC. The risk of BEC was thus foreseeable and the defendant was under a duty to guard against the harm eventuating. Its omission to do so was negligent in the circumstances.

- the defendant was the proximate cause of the plaintiff's loss in that it provided its own bank account details and was responsible for their accuracy and for the safety of their transmission. In failing to safeguard the safety of their transmission, the defendant acted wrongfully.

- as regards the element of wrongfulness, the plaintiff's loss in a case of this nature is both quantifiable and determinate and the risk of indeterminate liability as a policy consideration that militates against the recognition of liability for pure economic loss is thus averted

- that factual causation was established in that but for the negligent transmission by the defendant of its bank account details including its failure to inform the plaintiff, as depositor, of the dangers of BEC, the plaintiff would not have suffered the loss. Legal causation was likewise established as the negligent conduct of the defendant was linked sufficiently closely to the loss suffered by the plaintiff for legal liability to ensue, given that the loss was reasonably foreseeable under the circumstances.

Link to the full judgment - https://www.saflii.org/za/cases/ZAGPJHC/2023/14.html

Key takeaways from the judgment

- Organisations may be held delictually liable for cybercrimes on account of inadequate risk management.
- Clients ought to be sufficiently warned about business email compromise and/or any other attacks which may compromise an anticipated transaction.
- People are still the weakest link in the security chain. As it would appear from the judgment, even though the defendant had an Acceptable Use Policy in place which required that confidential/sensitive information must be password protected, there was never practice of what was preached by the Policy.
- The strength of an organisation's cybersecurity depends on the investment made on training employees and sensitizing clients.
- Electronic mail, professional as it may be, is an unsecure mode of communication.
- The technical safeguards for improving the security of electronic mail are rarely taken advantage, both at domain level and at application level.

For expert advice on how to avert the risks of business email compromise or email account compromise attacks, contact our well resourced team.

+267 316 7668
info@botlholelawgroup.co.bw