riman
RISK MANAGEMENT ASSOCIATION OF NIGERIA
Issue #75
April 2020

RISK Tips

Weekly Digest of Fundamentals of Risk Management

Helping You Understand Risk Management

Risk "Finally, we're seeing that nearly everyone understands security is a business risk issue at the end of the day. I joke with my clients, 'the board gets it, so they want to do something about cyber security, that's the good news.' But the bad news is, 'the board gets it and they want to do something about cyber security.' But of course it really is good news."
— Bruno Haring, Director, Cyber security & Privacy, PwC

New Cyber Risk Management Concerns for Directors & Officers

Never has senior management been faced with so many daily organizational threats stemming from computer-enabled perils. Risk management for protection of senior officers and the board has taken on new dimensions with unparalleled cybercrime and sweeping new data privacy regulations. The coronavirus pandemic compounds the challenge of maintaining computer security, as ever-growing numbers of workers follow directives to work from home.

Increasing Regulation and Oversight

The enactment of regulation like GDPR overseas has made cyber risk management increasingly difficult. Regulators now require that organizations have reasonably designed and implemented security around their online systems.

The Need for Directors' & Officers' Insurance

Directors' and officers' insurance has already been called upon to cover the significant costs of defense representation against shareholders and regulators over cyber incidents. D&O insurance is absolutely essential when the cyber stakes rise for officer and director liability exposures. Organizations cannot solely rely upon dedicated (standalone) cyber insurance products. Directors and officers will still need their D&O insurance protection since many cyber policies may impose an express exclusion for securities claims. Thus, noticing a cyber securities lawsuit for coverage under a cyber policy will surely trigger a coverage fight with many cyber insurance companies. It is therefore necessary in the ever more perilous cyber environment, it is essential that boards and the executive management team maintain the availability of D&O insurance for cyber-related claims.

Safeguarding D&O Insurance for Cyber Claims

With increases in cyber exposures for senior management, D&O insurance underwriters may begin to impose exclusions, sub-limits and other coverage conditions. In addition, policyholders need to be careful in responding to insurance applications that may be used by insurance companies post-claim to seek a forfeiture of coverage. They should also pay strict attention to D&O policy retroactive coverage dates. Where at all possible, push for better terms on this front. The problem is that some cyber threats occur well before the policyholder actually discovers evidence of an intrusion.

We now know all too well that hackers can intrude into computer systems weeks, months and even years before the policyholder becomes aware of the threat. Purchasing insurance coverage with a retroactive date that pre-dates the policy period, especially by a number of years, removes a potential coverage fight from the menu.

The following are some key risk management steps for board-level and officer cyber exposures:

• Stay informed about cyber exposures generally and your organization's security for online systems and storage devices specifically—these days, regulators and investors are demanding an informed executive suite in this area.

• Ensure that adequate resources are committed to combating the cyber threat. Cost-cutting here will not be well received when a serious breach has to be explained and defended to regulators, law enforcement, investors and other stakeholders.

•Ensure that reasonable steps are followed for telecommuting due to coronavirus, so that remote access and off-site data use is implemented and managed in as secure a manner as possible.

• Provide notice to your insurance companies quickly after a breach—including your D&O insurance companies. Early in the process of responding to a breach, the meter will be running on costs, and some of those costs may be to protect, investigate and defend the board.

• Ensure, in the first instance, that D&O insurance coverage (including primary, excess, etc.) remains free of cyber-related exclusions or sub-limits. Management will be highly concerned with any argued "gap" in coverage should a cyber event ensue—especially with the advent of cyber derivative shareholder litigation.

.

Source: RIMAN, Wikipedia, RIMS

RIMAN Upcoming Programmes

CRM Exam April Diet Stage 1, 2 & 3	Postponed Until Further Notice
Fundamentals of Risk Management	Postponed Until Further Notice

Kindly contact us on Tel: 0814 241 0241 or 0802 851 6377 email: info@rimanng.org, 15 Blessing Kayode Estate, Divine Mercy Close, Off Kayode Animashaun Street (Road 15), Off Admiralty Way, Lekki Phase 1, Lagos.
Follow us: Linkedin: rimanng Twitter:@rimanng Facebook: rimanng