iTOO[GO]
Claims Scenarios

CONTENTS

The digital world we operate in has seen a drastic transformation over the past few years. With **75% of companies impacted by a ransomware attack** and 80% bracing for the fallout from an email-borne attack and believing that their company is at risk due to inadvertent data leaks due to human error. **SMEs of all sizes are in the crosshairs for cyber-crime.**

Considering the ongoing threats posed by ransomware, BEC & other threats, here are some claims examples on how small businesses can fall victim to a cyber-attack.

Cyber extortion:

Meet Insuring Tomorrow (Pty) Ltd, an insurance broker with an annual revenue of approx. **R28 000 000** and around **2 500** clients.

Hackers gained unauthorized access to the Insuring Tomorrow network via a firewall vulnerability before their IT service provider could apply the security patch. With this access, the hackers stole Insuring Tomorrow's client data before encrypting their network.

The hackers demanded a double extortion (1. not to publish the stolen information and 2. to provide the keys to decrypt the data) of around **R7 500 000**

85%
increase in ransomware victims compared to 2020

144%
increase in average demand in 2021

78%
increase in average payment in 2021

Average ransom demand in 2021
OVER R35 000 000,

average ransom payment
OVER R8 500 000

Insuring Tomorrow's cyber policy was triggered and assisted with the following:

- IT incident response costs to assist with:
  - Determining how the hackers gained access to the environment
  - Containment of the incident and securing the environment
  - Investigating and engaging with the hackers to determine what data was stolen
  - Assisting with recovery of the environment from backups
  - Negotiating and communicating with the hackers to reduce the ransom demand
  - Ongoing dark web monitoring to check for publishing of the stolen data
  - Guidance on measures to implement to protect against future attacks
- Legal service provider costs to assist with:
  - Required notifications to the information regulator and other relevant regulatory bodies
  - Drafting of notifications to affected parties
- Crisis communications:
  - Costs for communications to the affected parties
  - As the incident did not break into the media there was not a requirement for public relations experts to respond to media enquiries and issue press statements
- Obtaining the required sanctions clearances to settle the ransom demand
- Settlement of the ransom demand to prevent the publishing of the client data
- Lost revenue as a result of the disruption to the operations

As the data was not published by the hackers, no ensuing litigation occurred. Had the data been published though and there was further litigation, Insuring Tomorrow's cyber policy would have provided cover for the defense and settlement of the litigation. The ultimate costs of the incident were just under **R2 500 000**.

A R5 000 000 insurance policy for Insuring Tomorrow (Pty) Ltd on the iTOO Go offering costs just under R1 960 per month.

Business Email Compromise (BEC):

Meet Legally Speaking Attorneys (Pty) Ltd, an attorney firm with an annual revenue of approx. **R5 000 000**

Hackers sent a Legally Speaking employee a phishing email, pretending to be from Office 365, requesting that they logon to their online profile to enable new security features. The link in the email took the employee to a fraudulent login page replicating the Office 365 login page, this page then stole their credentials where they attempted to login and directed them to the legitimate Office 365 login page. With the unauthorized mailbox access the hacker's setup forwarding rules on the mailbox forwarding all emails to the hackers' mailbox and allowing them to send emails as though they are from the compromised mailbox.

The hackers then altered an invoice sent to the employee and using the compromised mailbox sent this onto Legally Speaking's accountant. The accountant duly proceeded to make the payment of **R400 000** to the fraudulent account. By the time the incident was identified the funds could no longer be recovered.

According to a 2022 Mimecast study (State of Email Security),

94% of South African companies have been targeted in email-related phishing attacks in the past year. Most affected by these attacks are small and mid-sized businesses.

Legally Speaking Attorneys cyber policy was triggered and assisted with the following:

- IT incident response costs to assist with:
  - Determining how the hackers gained access to the mailbox
  - Investigating if any further fraudulent mails had been sent and which emails were sent to the hackers
  - Containment of the incident and securing the environment
  - Cleaning up and removal of the fraudulent mailbox rules
  - Assisting with the attempted recovery of the funds
  - Assistance on implementing multi factor authentication to prevent future compromises
- Legal service provider costs to assist with:
  - Required notifications to the information regulator and other relevant regulatory bodies
  - Assistance in drafting the communications to those who received fraudulent emails and whose emails had been forwarded onto the hackers
- Reimbursement of the funds lost

The ultimate costs of the incident were just under **R500 000**.

A R1 000 000 insurance policy for Legally Speaking Attorneys (Pty) Ltd on the iTOO Go offering costs just under R530 per month.

Insider malicious activity:

Meet Extreme Edge Engineering (Pty) Ltd, an engineering practice with an annual revenue of approx. **R150 000 000**.

A disgruntled employee at Extreme Edge found a new job but before leaving left some nasty code behind in their systems. 3 months after the employee left, the code triggered and adjusted tolerances on some of their machinery.

These adjustments resulted in damages to the manufacturing equipment, inability to use products being manufactured at the time and not being able to meet a client deadline.

Difficult to recover: 39% of SMEs don't have an incident response plan. 66% of SME's believe that they would not be capable of recovering from a cyber-attack.

Cyber Resilient Organization study by Resilient and IBM

Extreme Edge's cyber policy was triggered and assisted with the following:

- IT incident response costs to assist with:
  - Determining how the incident occurred
  - Containment of the incident and securing the environment
  - Ensuring the backups could be relied upon and then assisting with recovery of the environment from backups
  - Guidance on measures to implement to protect against future attacks
- Legal service provider costs to assist with:
  - Required notifications to the information regulator and other relevant regulatory bodies
  - Assisting with defense and settlement of ensuing litigation relating to the missed delivery
- Costs for repair to the damaged machinery and material costs for the damaged goods
- Lost revenue as a result of the disruption to the operations

The ultimate costs of the incident were just under **R10 000 000**.

A R10 000 000 insurance policy for Extreme Edge Engineering (Pty) Ltd on the iTOO Go offering costs just R3 350 per month.

Stolen device:

Meet Count on Us Accountants (Pty) Ltd, an accounting practice with an annual revenue of approx. **R35 000 000**.

Headed home from the office on a Friday afternoon a senior accountant stopped off to meet their family for dinner at their favorite local restaurant. Unfortunately, their car was stolen, including their laptop in the boot of the car. The laptop hard drive was not encrypted and contained sensitive information relating to clients currently being worked on.

Count on Us cyber policy was triggered and assisted with the following:

- IT incident response costs to assist with:
  - Confirming the data on the laptop
- Legal service provider costs to assist with:
  - Required notifications to the information regulator and other relevant regulatory bodies
  - Drafting of notifications to affected parties
- Identity theft monitoring for those whose data could potentially be compromised from the laptop to help prevent them suffering potential fraud against them
- Increased cost of working in recapturing and performing work that had been lost on the stolen laptop
- Lost revenue as a result of the disruption to the operations

Causes of Incidents:

13% Outdated Anti-virus

23% Outdated Firewall Patches

21% Poorly configured Firewall rules

44% Easy Guessable Passwords

15% Unsecured RDP Structures

As there is no proof of the data being stolen, no ensuing litigation occurred. Had the individuals whose data was stolen been the victim of fraud resulting from the stolen laptop, Count on Us cyber policy would have provided cover for the defense and settlement of the litigation. The ultimate costs of the incident were just under **R1 000 000**.

A R2 500 000 insurance policy for Count on Us Accountants (Pty) Ltd on the iTOO Go offering costs just under R1 365 per month.

Third party provider data theft:

Meet Smiley Faces Dentists (Pty) Ltd, a dental practice with an annual revenue of approx. **R20 000 000** and around **5 000** clients.

Smiley Faces Dentists make use of a third-party service provider to maintain their IT environment. The third-party service provider was the victim of a hack, the hackers utilized their access to gain unauthorized access to the Smiley Faces Dentists environment, allowing them to steal patient data and encrypt their systems.

The hackers demanded a double extortion equivalent to around **R12 500 000** not to publish the stolen information and to provide the keys to decrypt the data.

Smiley Faces cyber policy was triggered and assisted with the following:

- IT incident response costs to assist with:
  - Determining how the hackers gained access to the environment
  - Containment of the incident and securing the environment
  - Investigating and engaging with the hackers to determine what data was stolen
  - Assisting with recovery of the environment from backups
  - Negotiating and communicating with the hackers to reduce the ransom demand
  - Ongoing dark web monitoring to check for publishing of the stolen data
  - Guidance on measures to implement to protect against future attacks
- Legal service provider costs to assist with:
  - Required notifications to the information regulator and other relevant regulatory bodies
  - Drafting of notifications to affected parties
- Crisis communications:
  - Costs for communications to the affected parties
  - As the incident did not break into the media there was not a requirement for public relations experts to respond to media enquiries and issue press statements
- Obtaining the required sanctions clearances to settle the ransom demand
- Settlement of the ransom demand to prevent the publishing of the client data
- Lost revenue as a result of the disruption to the operations

As the data was not published by the hackers, the third-party provider paid the ransom, no ensuing litigation occurred. Had the data been published though and there was further litigation, Smiley Faces cyber policy would have provided cover for the defense and settlement of the litigation. The ultimate costs of the incident were just under **R7 500 000**.

A R7 500 000 policy for Meet Smiley Faces Dentists (Pty) Ltd on the iTOO Go offering costs just under R1 960 per month.

COVER OPTIONS

Below is an overview of the core cover provided in our iTOO Go offering and how SMEs can safeguard themselves against cyber risks:

First party

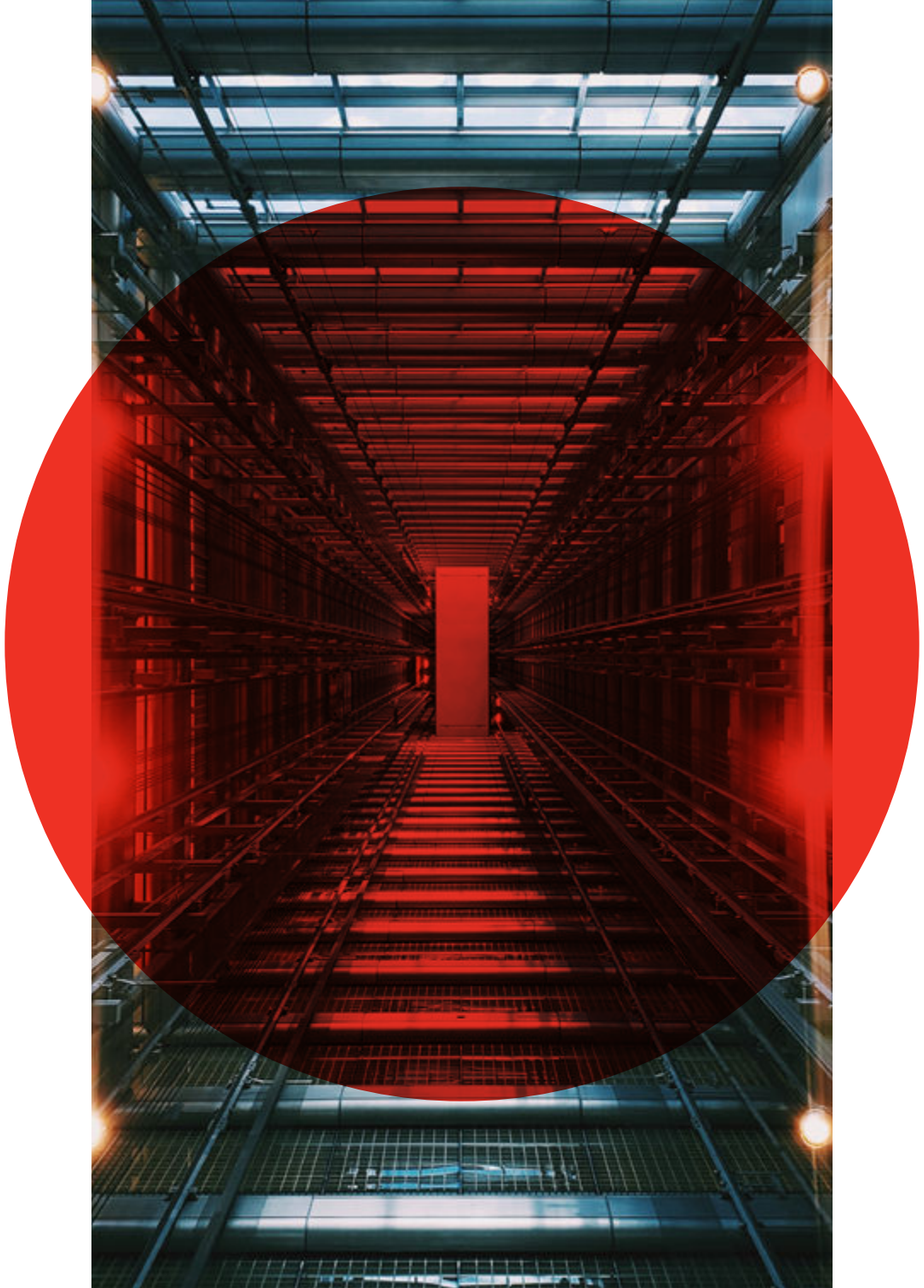
Business interruption loss of income and increased cost of working because of a systems security incident.

Data restoration costs to restore, re-collect or replace data lost, stolen or corrupted due to a systems security incident.

Regulatory fines to the extent insurable by law, fines imposed by a government regulatory body due to an information privacy breach.

Theft of funds unrecoverable loss of money, because of a system security incident by a third party.

Physical damage costs to replace or repair direct physical damage of property due to a system security incident.



Incident mitigation

Incident response costs to respond to a system's security incident, including:

- for professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, coordinating response activities, and making representation to regulatory bodies;
- to perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including data compromised, contain, mitigate, and repair the damage, and guidance on measures to prevent reoccurrence;
- for crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring;
- for communications to notify affected parties; and
- for remediation services such as identity theft monitoring to protect affected parties from suffering further damages.

Cyber extortion costs to investigate and mitigate a cyber extortion threat. Where required, 50% of the costs to comply with a cyber extortion demand.

Third party

Privacy liability defence and settlement of liability claims arising from compromised information.

Network security liability defence and settlement of liability claims resulting from a system security incident causing harm to third-party systems and data.

Media liability defence and settlement of liability claims resulting from disseminated content (including social media content) including unintentional defamation or copyright infringement

Optional coverage modules include:

Outsourced service provider cover for exposure from named outsourced service providers including business interruption losses.

Phone phreaking call and/or bandwidth usage costs because of unauthorised use of your telecommunications system by a third party.

Payment card industry fines and penalties cover for fines, penalties, assessments, chargebacks, reimbursements, and fraud recoveries which you become legally obligated to pay under a merchant services agreement.

This document is provided for information purposes only and should not be relied upon in assessing or determining coverage. Coverage for any claim is determined by the facts of the particular claim and the insurance policy wording as issued.

CONTACT US

For more information, please contact a member of our cyber team or your broker

- Ryan van de Coolwijk RyanV@itoo.co.za
- Lwando Cwane LwandoC@itoo.co.za
- Musa Khumalo MusawenkosiK@itoo.co.za

itoo.co.za
0861 00 4866