SAFEGUARDING YOUR BUSINESS

PRACTICAL CYBERSECURITY MEASURES

This guide provides businesses with straightforward steps to minimize the risk of email scams and to better understand the security issues related to Artificial Intelligence (AI). It also highlights the importance of including cybersecurity insurance as part of a comprehensive risk management strategy.

Matt Rose, CXO
Matt@TechRageIT.com
1511 East State Rd 434, Suite 2001
Winter Springs, FL 32708
407-278-5664

www.TechRageIT.com

Executive Summary

In today's digital world, businesses face tough cybersecurity issues. This guide offers simple ways to boost protection, focusing on email scams and AI security. It shares tips like improving email safety, training staff, and setting up secure transaction methods. It also covers how to keep AI systems safe by checking for weak spots and watching their outputs. The guide explains why cybersecurity insurance is vital for protecting finances from cyber threats. By following these steps, businesses can secure their operations, maintain customer trust, and promote steady growth. This document is a key resource for leaders wanting to improve their cybersecurity defenses.

What is BEC?

Business Email Compromise (BEC) is a sophisticated scam targeting businesses that conduct wire transfers and have suppliers abroad. Cybercriminals compromise legitimate email accounts through social engineering or hacking to conduct unauthorized transfers of funds.

100%

Increase

There are several studies showing that Business Email Compromise attacks have great success rates. To that, the FBI reported that between June 2016 and July 2019 there was a 100% increase in identified losses due to BEC Scams.

Impact On Business

FINANCIAL LOSS

$1.8 billion

According to the FBI, BEC scams resulted in $1.8 billion in losses in 2020 alone.

COMPROMISED SENSITIVE INFORMATION

80%

Over 80% of businesses affected by BEC also report data breaches that expose sensitive company and customer information.

REPUTATIONAL DAMAGE

41%

A report by Hiscox indicates that 41% of companies that experience cyber incidents report reputational harm, which can lead to loss of business and customer trust.

Enhance Email Security

- Implement multifactor authentication (MFA) for email accounts.
- Use email filtering tools to identify and block suspicious emails.

Train Employees

- Conduct regular training on recognizing phishing attempts.
- Encourage verification of any changes in account details or requests for transactions.

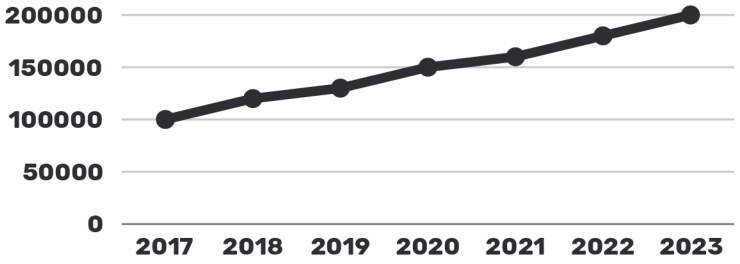
Establish Clear Protocols

- Develop and enforce a company-wide policy for financial transactions.
- Require dual approval for significant fund transfers.

Cybersecurity Insurance

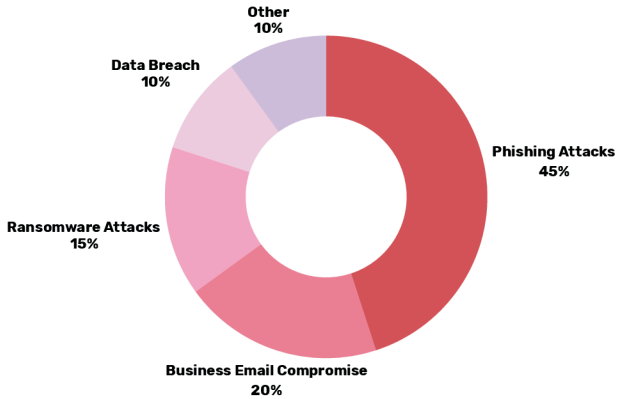
Cybersecurity insurance is a vital part of risk management, offering financial protection against the costs of cyber incidents like data breaches and ransomware attacks. It helps cover expenses such as data recovery, legal fees, and customer notifications.

Businesses should assess their specific risks to ensure policy coverage aligns with their needs, and consulting an insurance advisor can aid in selecting the right coverage, providing peace of mind against evolving threats.



Average cost of cyber incidents over time.

Sources: Verizon DBIR, FBI IC3, CISA, Ponemon Institute, Symantec



Sources: Verizon DBIR, FBI IC3, CISA, Ponemon Institute, Symantec