Wolfpack Logo Update 2020(Red)(Hi-Res)

Wolfpack Information Risk provides specialist information and cyber threat consulting, training, awareness and incident support services to African governments and organisations.

WOLFPACK CARES. We are passionate defenders of communities, companies, and countries against cyber threats.

Wolfpack-Newsletter-Header-Community-cyber-safety-is-our-concern

Greetings Cyberwolves

Business Email Compromise (BEC) is a perplexing problem facing our people, processes, and technologies. BEC exploits the fact that so many of us rely on email to conduct business in our personal and professional capacities.

This global problem targets organisations of all sizes across every industry worldwide. Email communication continues to be a huge security headache for cybersecurity professionals, and even the most astute organisations fall victim to these sophisticated email threats. BEC can cost a company millions in lost revenue, reputational damage, and disruption to daily lives.

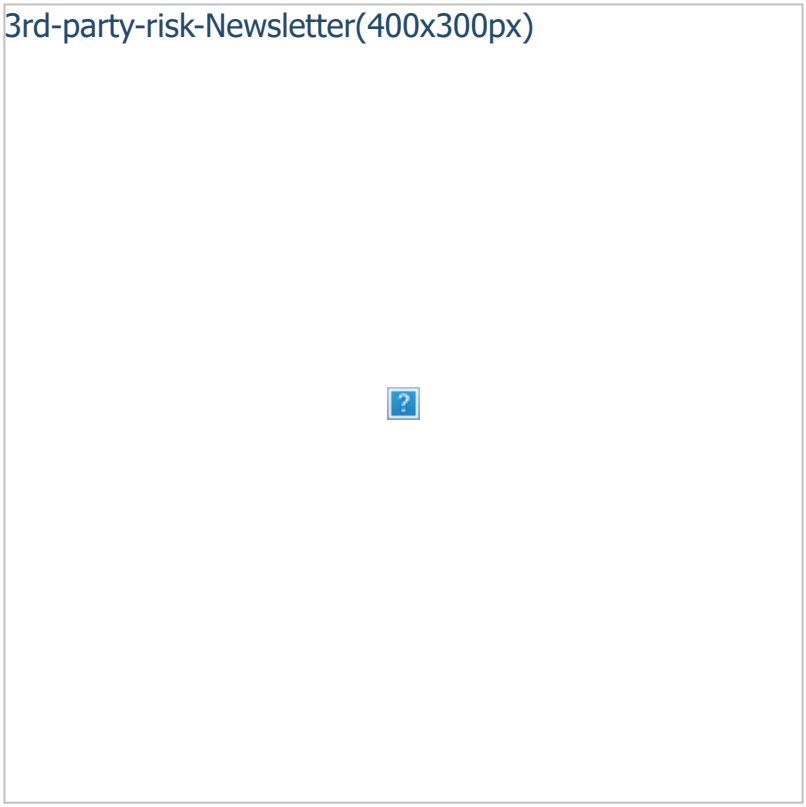
Organisations are being compromised in one way or the other. Third-party supplier risk vulnerabilities also contribute to these threats. It is vitally important for Small to Medium Enterprises (SMEs) to shift their perspective and prepare for these threats. Most SMEs believe that hackers will not target their organisation because they are small, or if their penetration test is good, they are "unhackable". Such SMEs need to stop believing these cyber myths and start preparing for them.

BEC vulnerabilities always catch unsuspecting humans, making the weakest link even weaker. Cybersecurity culture plays a vital role in setting the standards for behaviour throughout an organisation and helps to integrate security skills and awareness into the company culture.

BEC is subtle yet dangerous. A chain is only as strong as the weakest link, and the same applies to a company's cybersecurity posture. It is our business to protect our business's business.

Yours Securely
#protectioninthepack

ADVISORY & CYBERSECURITY



Wolfpack's Head of Advisory, Steve Simmonds, has shared his insights regarding third-party supplier risk vulnerabilities to organisations and how they can ensure that preventative, detective, and investigative controls are in place. Here are his insights:

- **Attack surface expansion**: On average, 60% of workers are remote, and some may never return to the office. This leaves organisations more vulnerable to attack.
- **Identity system defence:** Identity systems are coming under sustained attack. Misuse of credentials is now a primary method that attackers use to access systems and achieve their goals.
- **Digital supply chain risk**: Security and risk management leaders must partner with other departments to prioritise digital supply chain risk and pressure suppliers to demonstrate security best practices.
- **Awareness:** Human error continues to feature in most data breaches, showing that traditional approaches to security awareness training are ineffective. Companies should consider implementing behaviour and culture change programs designed to provoke more secure ways of working.

CISO Ed and Co cartoon

The Adventures of CISO Ed & Co attempts to highlight the everyday frustrations, heroism, and insights of CISOs and infosec teams while bringing some fun to the serious business of cybersecurity. We hope CISO Ed & Co. brings a grin to your face as you go about your day. **Compliments of Balbix**

TRAINING, AWARENESS & RESOURCING

Business Email Compromise Recovery Poster1_V0.3

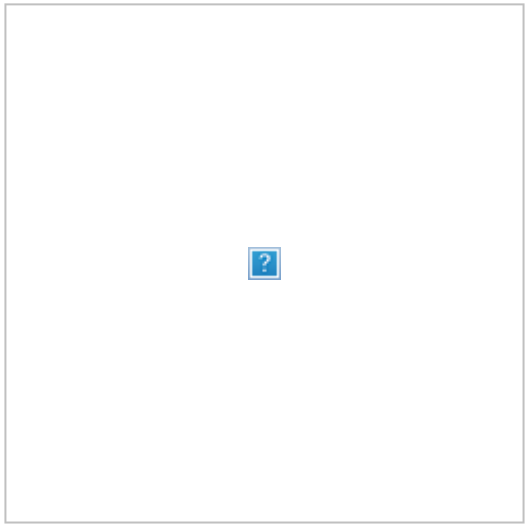
Now that you have survived a Business Email Compromise (BEC) incident, you should always keep it in the back of your mind to shift your perspective when checking emails. Here is a poster which includes some useful tips to help with your recovery.

#protectioninthepack #businessinjuly #businessemailcompromise

OUR PARTNERS

Social media and digital engagement have created inherent trust between connected users that attackers seek to capitalise on. Fake accounts impersonating brands and executives have become more common across social media in recent years across industries. With the success of these attacks, bad actors have applied similar tactics to other vectors, such as email. **READ MORE**

Most companies use security testing for compliance to take stock of their security across the organisation and report results to an internal or external auditor. Low-quality reports, long cycles to deploy tests, employee burnout, frequent code releases, and tester schedules can make this process cumbersome. Over 40% of organisations outsource their security testing function to augment their internal teams and improve results. **READ MORE**



Stay informed and become a pack member by following us on LinkedIn, Twitter, and