WOLFPACK STORY

Wolves belong to family groups called packs, usually consisting of eight to fifteen members. Within the pack, each member has a particular set of skills and responsibilities, which are executed with purpose and precision.

Environmental Analysis

Before wolves go in for the kill, they spend a considerable amount of time studying their prey. Wolves are masters at understanding environmental conditions and making the best strategic decisions based on the intelligence they have gathered.

Wolfpack has developed a comprehensive health check that considers all key technology people and business requirements and thereafter, provides a tailored strategy and roadmap for each customer. A one-size-fits-all approach does not work.

Built for the Kill

Wolves will defend their territory and work together to fend off much larger predators. Although not as physically strong as other predators in their habitat, wolves hunt in packs to kill prey that is both larger and stronger than each individual wolf. Teamwork allows the pack to target larger prey that a lone wolf would fail to kill.

No single country, government or organisation can effectively protect themselves against the vast barrage of cyber threats. Wolfpack’s underpinning culture has been forged through national and industry community initiatives and is committed to the improvement of cyber collaboration and security within the African continent and beyond.

The Wolf Howl

The wolf howl is a distinct call to action for all members of the pack. Howling helps the wolf pack to communicate effectively in thickly forested areas or over vast distances and to summon members when they are attacked. Wolves will also howl for communal reasons. Some scientists and environmentalists surmise that such pack sessions strengthen the wolves’ social bonds and camaraderie; similar to choral singing among humans.

“A true partnership model is one that leverages the strengths of internal resources, trusted outside specialists and industry or global collaboration initiatives. This is pivotal to provide assurance that the required risk management, threat intelligence, monitoring, incident management and business resilience building blocks are in place to support organisational requirements.”

Our Services:

- Research and Threat Intelligence – International cyber security research projects and local insight into strategic and operational cyber threats facing companies
- Advisory – Professional business aligned information risk services
- Awareness – Establishing a security-aware culture throughout the organisation
- Training – Tailored training programmes to ensure optimal skills-transfer
- Managed Services – Cyber Threat Monitoring Centre offering threat and vulnerability management services
- Incident Management – Proactive and reactive incident response services

Protection in the Pack

WOLFPACK INFORMATION RISK (PTY) LTD

We are an independent information risk services company

Established: June 2011

We specialise in information and cyber threat management covering the full spectrum of prevention, detection, incident response and business resilience capabilities

“The Wolf Pack”

“Protection in the Pack”

WOLFPACK INFORMATION RISK (PTY) LTD

We are an independent information risk services company

Established: June 2011

We specialise in information and cyber threat management covering the full spectrum of prevention, detection, incident response and business resilience capabilities

“Protection in the Pack”

WOLFPACK INFORMATION RISK (PTY) LTD

We are an independent information risk services company

Established: June 2011

We specialise in information and cyber threat management covering the full spectrum of prevention, detection, incident response and business resilience capabilities

“The Wolf Pack”

“The Wolf Pack”

WOLFPACK INFORMATION RISK (PTY) LTD

We are an independent information risk services company

Established: June 2011

We specialise in information and cyber threat management covering the full spectrum of prevention, detection, incident response and business resilience capabilities

“The Wolf Pack”

“The Wolf Pack”

WOLFPACK INFORMATION RISK (PTY) LTD
The Benefits and Risks of Cyberspace

The cyber age is introducing rapid change and business disruption including:

- Untapped global customer markets
- Faster supply chain integration
- New tools to enhance productivity and collaboration
- Reduced digital storage costs
- Mobility and much more.

The cyber age has furthermore disrupted business models of traditional organisations at a rate never experienced before.

And it Doesn’t Appear to be Slowing Down

We all now operate in an interconnected cyber ecosystem. As a result, securing critical business and personal information, transactions and operations, means looking beyond the walls of the organisation.

The New Reality Facing all Connected Organisations

- A massive reliance on technology
- Transactions and operations span multiple entities
- Increased demand for technology means that skills are scarce and expensive
- Organisations are expected to provide trust and privacy: ignorance is no longer accepted as an excuse
- A large increase in threat actors abusing technology to further their own agendas

The Cyber Paradox

A massive reliance on technology
Transactions and operations span multiple entities
Increased demand for technology means that skills are scarce and expensive
Organisations are expected to provide trust and privacy: ignorance is no longer accepted as an excuse
Mobility and much more.

The cyber age has furthermore disrupted business models of traditional organisations at a rate never experienced before.

And it Doesn’t Appear to be Slowing Down

We all now operate in an interconnected cyber ecosystem. As a result, securing critical business and personal information, transactions and operations, means looking beyond the walls of the organisation.

The New Reality Facing all Connected Organisations

- A massive reliance on technology
- Transactions and operations span multiple entities
- Increased demand for technology means that skills are scarce and expensive
- Organisations are expected to provide trust and privacy: ignorance is no longer accepted as an excuse
- A large increase in threat actors abusing technology to further their own agendas

Good Cyber Security = A Healthy Business

Weak Cyber Security = A High Risk Business

Organisations are facing increased exposure to cyber risk. Cyber threats should be prioritised as a key enterprise risk. Boards should be briefed on the potential impact to the organisation and obtain assurance that risks are appropriately monitored and managed. Boards and executives that maintain their focus on information risk management do more than protect the business; they enable growth in the digital age.

Good Cyber Security = A Healthy Business

Weak Cyber Security = A High Risk Business
Attacks against countries, organisations and individuals are on the increase.

**THREAT LANDSCAPE**

- Governments
- Competitors/ Clients
- Hackers
- Employees
- Country Risk
- Organisation Risk
- People Risk

**Estimated Cost of Cybercrime**

- **$400 Billion+**

---

**CYBERCRIMINAL CODE OF ETHICS**

"If what you put on the Internet is worth anything, one of us will try to hack or steal it."

"If we can't sell it, we'll just encrypt it or erase it so you can't use it or simply post it online to ruin your reputation."

"If you don't care about protecting your stuff from the likes of us, don't worry: You're our favourite type of customer!"

---

**WOLFPACK INFORMATION RISK (PTY) LTD**
THE WOLFPACK 7 POINT EXECUTIVE CHECKLIST

1. Assess the Risk
   - Cyber resilience today should be a key focus of boards and senior management. Do you know where your organisation is exposed?

2. Understand the Impact
   - Determine the operational, financial and reputational harm to your organisation should you be the victim of a major breach or disruption.

3. Establish an Effective Information Risk Improvement Programme
   - Use recognised international guidance coupled with local assurance reviews.

4. Implement a Tailored Training and Awareness Programme
   - Address the specific risk and skill gaps in your organisation. Lead by example.

5. Incident Management
   - Ensure you have an organisation-wide incident response team and effective plans which are tested at regular intervals.

6. Monitor
   - Institute consistent board oversight of programme milestones and metrics to ensure effective risk management.

7. Ensure Business Resilience Requirements
   - Redundancy and backup systems, disaster recovery, business continuity and crisis management should be in place.

CASE STUDY: HOW REINTRODUCING WOLVES HELPED SAVE A NATIONAL PARK

Wolves were once the top predator in America’s world-famous Yellowstone National Park, but the population was eradicated in the 1920s. In 1995, a small pack of wolves were reintroduced to Yellowstone to manage the negative effects of overgrazing by a rising elk population. The effect amazed scientists and dramatically changed the park’s rivers, forests and the landscape itself. Click the box to watch this amazing short documentary.

INTRODUCING THE "WOLFPACK EFFECT" INTO YOUR ORGANISATION

Wolfpack works with the management teams of their clients to securely unlock the operational and financial benefits that modern technology and cyberspace have to offer. Our holistic approach combined with your team’s support will maintain the sensitive balancing act between business needs and effective information risk management. We cover the full spectrum of prevention, detection, incident response and business resilience requirements.

This section outlines our approach as we jointly undertake the journey to improve the maturity of information risk management across the organisation.
The purpose of an information risk strategy and framework is to determine how to recognise, manage and decrease the impact of information and cyber risks effectively, and in a repeatable manner.

This will be tailored to the industry, size, industry risk profile and culture of the organisation and informed by the constantly changing cyber threat and vulnerability landscape.

Effective governance structures reinforce accountability by defining clear responsibilities and lines of reporting and escalation.

Cyber security compliance requirements need to be identified and addressed. Non-compliance can incur a financial penalty or incur a breach that could cause financial harm or penalties, incure an incident or affect an employee’s job. Ongoing monitoring of these issues will help determine the cyber resilience of the organisation and guide the design, implementation, and effectiveness of related information risk programmes.

As part of the enterprise risk management capability, the organisation should evaluate the inherent risk presented by people, processes, technology, and underlying data that supports each identified business unit, activity, and service. All functions should then identify and assess the existence and overall effectiveness of controls to protect the organisation’s assets. The combination of these will determine an acceptable residual risk.

In alignment with the organisation’s strategic and business objectives, the organisation should evaluate the risk tolerance of the organisation and determine an acceptable residual risk.

Information protection needs to be implemented across our people, process and technology domains.

A clear majority of breaches are due to human involvement, either malicious or accidental and not due to a lack of technology protection and controls.

Business culture plays a significant role in setting the standards for acceptable risk in the organisation. Startlingly, 90% of employees believe they are the least likely person to be targeted by a cybercriminal. As such, the people aspect of information security requires a strong focus on information security awareness.

Effective governance structures reinforce accountability by defining clear responsibilities and lines of reporting and escalation.

Cyber security compliance requirements need to be identified and addressed. Non-compliance can incur a financial penalty or incur a breach that could cause financial harm or penalties, incure an incident or affect an employee’s job. Ongoing monitoring of these issues will help determine the cyber resilience of the organisation and guide the design, implementation, and effectiveness of related information risk programmes.
Wolfpack has developed a robust approach (AIM) to address an organisation’s specific business, governance, risk and compliance requirements across the vast domain of information risk.

**ASSESS**

- Identify the specific information threats facing your business environment
- Validate acceptable information risk levels in accordance with business requirements
- Determine the maturity of existing information risk people, process and technology controls across key domains
- Highlight key vulnerabilities and risk areas across the organisation

**IMPROVE**

- Institute a robust information risk improvement programme
- Information risk strategy
- Tactical priority roadmap for the establishment of an information risk management framework
- An operational improvement programme in accordance with international specifications
- This includes a tailored training and awareness programme to ensure skills transfer

**MONITOR**

- Connecting your organisation to cyberspace makes it vulnerable to the full spectrum of global threats and requires constant monitoring indicators of possible global threats and compromises
- Technical - Correlate and analyse event data, determine suspicious network behaviour, conduct active network scanning and respond to threats more effectively
- Business and Human Risk - Monitor online activity risks for business, social media and human environments
- Performance Measurement - Ensure the performance of the programme aligns to support business objectives
Governance, Risk and Compliance Services

IT governance is a framework that ensures your IT infrastructure supports and enables an organisation to achieve its goals. We will perform an IT process maturity review, IT risk assessment and can assist with remediation of your IT environment.

IT Governance and IT Risk Review
Organisations are expected to safeguard personal information entrusted to them; ignorance is no longer accepted as an excuse. We conduct a privacy impact assessment and provide the necessary consulting services to ensure your organisation is compliant with relevant privacy and data protection requirements.

We will review your current supplier management lifecycle to ensure that the applicable governance components such as NDAs, SLAs and other contracts are in line with information risk management requirements. We also perform independent third-party risk assessments.

IT change and release management is primarily concerned with the governance of transitioning new technology and procedural adjustments into a live operational environment, with as little risk as possible.

Following an alignment process to the BCM strategy, we will establish the required BCM governance components in line with the business objectives. We then conduct a Business Impact Analysis (BIA) with senior management teams to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Our information risk framework provides the foundation upon which we architect the strategy to support business objectives and the subsequent information risk programme. The modular nature of the framework further provides an agile environment to allow the organisation to continuously re-evaluate their priorities and approach as the business and threat landscape evolves.

We will review your current IM, DR and BCM environment and ensure an ISO 27035 aligned incident management programme is in place to handle major privacy or cyber incidents. We provide the necessary governance documentation, detailed ‘battle guides’ and training / simulated incident testing for the Incident Response Team (IRT).
We have successfully run training programmes for the banking and government sector. Based on specific industry or country needs we are able to structure a course tailored to your specific requirements.

Simulations are online interactive lessons where a student has to navigate their way through the course and make the correct decisions. This is an effective way to check how a student will act in a real life situation.

There is often a disconnect between policy writers and their audience. We have summarised key requirements from a typical information security policy into an easy to read, branded story booklet available in digital format that can be shared electronically or printed, which outlines expected behaviours.

We have successfully run training programmes for the banking sector.

A large portion of incidents are due to human involvement, which may be malicious or accidental and not a lack of technology protection. Culture plays a huge role in setting the standards for behaviour throughout an organisation, starting with all levels of management and with each employee or third-party involved in the organisation. Wolfpack provides a full turnkey awareness solution that includes business needs analysis, content development and customisation, programme management, an intuitive learning management system, as well as various human vulnerability assessments conducted using our online threat platform Camo Wolf.

We have an online threat assessment platform that can be used to conduct realistic attack scenarios on teams within your organisation. We are able to conduct spear-phishing, bad actors use a combination of interactive feedback technology and "eye-opening" demonstrations and are extremely effective at getting "buy-in" from your users.

Workshops teach your employees how to protect themselves and their families against relevant cyber threats when using social media, mobile devices, games etc. The workshops use a combination of interactive feedback technology and "eye-opening" demonstrations and are extremely effective at getting "buy-in" from your users.
Security Information and Event Management (SIEM) – Correlate and analyse security event data from across your network.

Behavioural Monitoring – Identify suspicious behaviour on your assets.

Asset Discovery – Determining what devices are connected on the network.

Vulnerability Assessment and Intrusion Detection – Discover and monitor your crown jewel assets for weaknesses and possible compromise.

Online Brand Reputation Management

Facebook and LinkedIn auto content moderation and domain protection from takeover, fake spoofing, fraud/scams, counterfeit, violence, phishing, inappropriate use.

Social Media Protection

We have relationships with local and international partners to assist our clients with an incident response service thereby giving you access to a highly-experienced incident response specialist, at the time when you need it most.

Cyber Incident Response

One of the challenges highlighted at previous CyberCon events was the lack of a national awareness programme. Wolfpack partnered with the British High Commission to build Alert Africa to provide guidance on cyber threats and provide a portal to report a cybercrime in South Africa.

Alert Africa Community Awareness Website

Wolfpack’s culture is one of community engagement and support. As such we undertake a number of pro bono projects each year.

Wolfpack Cares Social Responsibility Projects

Wolfpack has conducted a number of national or sector-specific related threat research projects on topics such as cybercrime and critical information infrastructure protection. Our research is 100% vendor-neutral and is aimed at providing guidance to policy makers and strategic public and private sector stakeholders.

National and Industry Research Programmes

Wolfpack is the event manager of the CyberCon Africa conferences hosted in Gauteng, South Africa. The purpose of the conference is to collaborate to identify national cyber vulnerabilities facing the continent and to jointly work on finding solutions.

CyberCon Africa Annual Cyber Conference

One of the challenges highlighted at previous CyberCon events was the lack of a national awareness programme. Wolfpack partnered with the British High Commission to build Alert Africa to provide guidance on cyber threats and provide a portal to report a cybercrime in South Africa.

Alert Africa Community Awareness Website

Wolfpack’s culture is one of community engagement and support. As such we undertake a number of pro bono projects each year.

Wolfpack Cares Social Responsibility Projects

Wolfpack has conducted a number of national or sector-specific related threat research projects on topics such as cybercrime and critical information infrastructure protection. Our research is 100% vendor-neutral and is aimed at providing guidance to policy makers and strategic public and private sector stakeholders.

National and Industry Research Programmes

Wolfpack is the event manager of the CyberCon Africa conferences hosted in Gauteng, South Africa. The purpose of the conference is to collaborate to identify national cyber vulnerabilities facing the continent and to jointly work on finding solutions.

CyberCon Africa Annual Cyber Conference

One of the challenges highlighted at previous CyberCon events was the lack of a national awareness programme. Wolfpack partnered with the British High Commission to build Alert Africa to provide guidance on cyber threats and provide a portal to report a cybercrime in South Africa.

Alert Africa Community Awareness Website

Wolfpack’s culture is one of community engagement and support. As such we undertake a number of pro bono projects each year.

Wolfpack Cares Social Responsibility Projects
Wolfpack has partnered with a number of local and international organisations, which complement our service offerings.

**PECB** is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including but not limited to Information Security, IT, Business Continuity, Service Management, Quality Management Systems, Risk and Management, Health, Safety and Environment. Wolfpack Information Risk is an authorised PECB training partner and holds multiple professional PECB certifications.

**CompTIA** is the voice of the world’s information technology (IT) industry. As a non-profit trade association advancing the global interests of IT professionals and companies, they focus their programmes on four main areas: education, certification, advocacy, and philanthropy. Wolfpack Information Risk is an authorised CompTIA training partner.

The Services SETA Education and Training Quality Assurance Body (ETQA) has been accredited by SAQA for performing all quality assurance functions with regard to the implementation of learning programmes that falls within the services sector’s scope. Following a stringent assessment in 2012, Wolfpack Information Risk was accredited as a skills development provider to offer outcome-based learning programmes.

Wolfpack is a Managed Services Solution Provider (MSSP) for AlienVault in South Africa. Their Unified Security Management (USM) solution combines 5 key security capabilities with expert threat intelligence that is updated from the Open Threat Exchange (OTX). Every day, AlienVault Labs analyses an immense amount of data submitted to OTX by more than 37,000 participants from 140+ countries.

Wolfpack is a Managed Services Solution Provider (MSSP) for ZeroFOX in Africa. They deliver automated threat detection and remediation across social, mobile, digital, and collaboration platforms. ZeroFOX identifies organisational risks and security threats targeting both businesses and employees.
CONTACT US

@ Email
info@wolfpackrisk.com

💰 Phone
+27 11 794 7322

🌐 Website
https://www.wolfpackrisk.com