HAWK RISK PROTECTION

Cyber Security & Investigations

www.dcii-hawkrisk.co.za

HAWK RISK PROTECTION
OFFERS CUTTING-EDGE CYBER SECURITY SOLUTIONS

1

Why you need Cyber Security

Hawk Risk Protection offers a comprehensive way of protecting your valuable data from modern day threats which is vital – no matter your business' size or industry.

Cybersecurity is the practice of protecting computer systems, networks, and data from cyber threats

1 What is protects

Devices like computers, laptops, tablets, and smartphones, as well as online services like email, online shopping, online banking, and social media.

2 What it prevents

Unauthorized access, theft, damage, or disruption of systems, networks, and data.

3 How it is accomplished

Through technologies, processes, and controls that reduce the risk of cyber attacks.

4 Cybersecurity is important because

- More and more of our lives are online
- The complexity of information systems and the societies they support
- The growth of smart devices like smartphones and televisions

5 Fields that need cyber security

Cybersecurity roles are available in many different fields, including: Education, Financial services, Government, Healthcare, Manufacturing, and Mining.

Danie Booyens • +27 71 212 5715 • danie@dcii-hawkrisk.co.za • www.dcii-hawkrisk.co.za

2

Types of Cyber Security

1 Network Security

Most attacks occur over the network, and network security solutions are designed to identify and block these attacks. These solutions include data and access controls such as Data Loss Prevention (DLP), IAM (Identity Access Management), NAC (Network Access Control), and NGFW (Next-Generation Firewall) application controls to enforce safe web use policies.

Advanced and multi-layered network threat prevention technologies include IPS (Intrusion Prevention System), NGAV (Next-Gen Antivirus), Sandboxing, and CDR (Content Disarm and Reconstruction). Also important are network analytics, threat hunting, and automated SOAR (Security Orchestration and Response) technologies.

2 Cloud Security

As organizations increasingly adopt cloud computing, securing the cloud becomes a major priority. A cloud security strategy includes cyber security solutions, controls, policies, and services that help to protect an organization's entire cloud deployment (applications, data, infrastructure, etc.) against attack.
While many cloud providers offer security solutions, these are often inadequate to the task of achieving enterprise-grade security in the cloud. Supplementary third-party solutions are necessary to protect against data breaches and targeted attacks in cloud environments.

3 Endpoint Security

The zero-trust security model prescribes creating micro-segments around data wherever it may be. One way to do that with a mobile workforce is using endpoint security. With endpoint security, companies can secure end-user devices such as desktops and laptops with data and network security controls, advanced threat prevention such as anti-phishing and anti-ransomware, and technologies that provide forensics such as endpoint detection and response (EDR) solutions.

4 Mobile Security

Often overlooked, mobile devices such as tablets and smartphones have access to corporate data, exposing businesses to threats from malicious apps, zero-day, phishing, and IM (Instant Messaging) attacks. Mobile security prevents these attacks and secures the operating systems and devices from rooting and jailbreaking. When included with an MDM (Mobile Device Management) solution, this enables enterprises to ensure only compliant mobile devices have access to corporate assets.

HAWK RISK PROTECTION

5 IoT Security

While using Internet of Things (IoT) devices certainly delivers productivity benefits, it also exposes organizations to new cyber threats. Threat actors seek out vulnerable devices inadvertently connected to the Internet for nefarious uses such as a pathway into a corporate network or for another bot in a global bot network.

IoT security protects these devices with discovery and classification of the connected devices, auto-segmentation to control network activities, and using IPS as a virtual patch to prevent exploits against vulnerable IoT devices. In some cases, the firmware of the device can also be augmented with small agents to prevent exploits and runtime attacks.

6 Application Security

Web applications, like anything else directly connected to the Internet, are targets for threat actors. Since 2007, OWASP has tracked the top 10 threats to critical web application security flaws such as injection, broken authentication, misconfiguration, and cross-site scripting to name a few.

With application security, the OWASP Top 10 attacks can be stopped. Application security also prevents bot attacks and stops any malicious interaction with applications and APIs. With continuous learning, apps will remain protected even as DevOps releases new content.

7 Zero Trust

The traditional security model is perimeter-focused, building walls around an organization's valuable assets like a castle. However, this approach has several issues, such as the potential for insider threats and the rapid dissolution of the network perimeter.

As corporate assets move off-premises as part of cloud adoption and remote work, a new approach to security is needed. Zero trust takes a more granular approach to security, protecting individual resources through a combination of micro-segmentation, monitoring, and enforcement of role-based access controls.

Danie Booyens • +27 71 212 5715 • danie@dcii-hawkrisk.co.za • www.dcii-hawkrisk.co.za

Cyber Threats

The cyber threats of today are not the same as even a few years ago. As the cyber threat landscape changes, organizations need protection against cybercriminals' current and future tools and techniques.

Gen V Attacks	Large-scale, multi-vectors attacks
Supply Chain Attacks	Attacks from third-party software or access
Ransomware	Many cybercrime groups have access to advanced malware
Phishing	Most common and effective means by which cybercriminals gain access to corporate environments
Malware	Modern malware is swift, stealthy, and sophisticated and requires cyber security solutions focused on prevention

4 Our Cyber Security Solutions

Save time and money and improve resilience with cybersecurity and data protection. We offer a complete cyberthreat defence in one solution.

☑ All-in-One Protection

Our software natively integrates backup with cybersecurity and endpoint management to provide end-to-end cyber resilience.

☑ Secure Backup & Recovery

Strengthen business resilience with secure, immutable backup, rapid recovery and anti-ransomware technologies.

☑ Comprehensive Security Capability

Ensure peace of mind and help to avoid costly downtime with integrated endpoint detection and response (EDR) and automated URL filtering.

☑ Powerful Endpoint Management

Minimise outages and boost uptime with automatic anomaly detection, proactive patching, automated scripts, and remote access for troubleshooting.

☑ Anti-Malware & Antivirus

Proactively protect your data, applications and systems from advanced cyberattacks with real-time protection, AI-enhanced behavioural heuristic antivirus, anti-malware, anti-ransomware and anti-cryptojacking technologies

☑ Fail-Safe Patching

Our software automatically creates a backup before any patches are applied to ensure that its quick and easy to recover if any installed patches cause system instability.

☑ Forensic Backup

Simplify future analysis, compliance reporting and investigations by collecting digital evidence – like memory dumps and process information – from disk-level backups.

☑ Defeat Ransomware

Prevent reinfection via integrated anti-malware scanning and malware removal during the recovery process. Gain peace of mind with immutable backup storage.

Danie Booyens • +27 71 212 5715 • danie@dcii-hawkrisk.co.za • www.dcii-hawkrisk.co.za

Get in Touch

DANIE BOOYENS
MANAGING DIRECTOR
+27 71 212 5715
danie@dcii-hawkrisk.co.za
www.dcii-hawkrisk.co.za