ISRM

THE INSTITUTE OF STRATEGIC
RISK MANAGEMENT

FROM SNAKES TO DRAGONS: **UNDERSTANDING RISK IN MODERN SECURITY ENVIRONMENTS**

by Ben Griffin F.ISRM

INTRODUCTION

Organisations today operate in increasingly complex risk environments where traditional security approaches are often insufficient to address evolving threats.

In most organisations, security problems tend to look familiar.

A door that should have been locked wasn't

An access badge that should have been cancelled remained active.

A procedure that should have been followed wasn't.

These failures are frustrating, but they are also relatively straightforward. They are localised problems with identifiable causes and clear corrective actions.

For decades, most security systems have been built around identifying and removing exactly these types of risks.

And for those situations, the traditional tools of security work well.

Audits, inspections, procedures, and compliance monitoring are effective ways to find problems and correct them before they escalate.

But the risk environments organisations now operate in are becoming far more complex.

Some threats involve coordinated groups exploiting weaknesses across multiple parts of an operation. Others evolve rapidly in response to defensive measures. And occasionally, events occur that disrupt entire industries.

Put simply, the risks organisations face today do not all behave in the same way.

Some behave like simple hazards that can be removed once identified.

Others behave more like predators within an ecosystem.

THE FIVE CREATURES OF RISK

If we look at modern risk environments through this ecological lens, a useful pattern begins to emerge.

Different threats behave in fundamentally different ways. Some appear as isolated operational failures that can be corrected once identified. Others involve coordinated actors exploiting systemic weaknesses. Some evolve in response to defensive measures, while a small number have the potential to disrupt entire industries.

Recognising these differences is essential because each type of threat demands a different kind of response.

For practical purposes, these patterns can be grouped into five broad categories of risk that organisations must learn to recognise and manage.

THE SNAKE SIMPLE RISK

Snakes represent the traditional risks that most security systems were designed to address.

These are isolated problems with clear causes and relatively straightforward solutions.

Examples include broken locks, access control failures, unattended bags, missing identification, or procedural errors. They are visible, localised, and usually solved through inspection, enforcement, or corrective action.

Compliance systems work well here. Audits, checklists, and procedures are effective tools for identifying and removing these kinds of threats.

For snakes, traditional security works.

The problem is that modern organisations rarely face snakes alone.

THE WOLF COORDINATED RISK

Wolves represent coordinated threats involving multiple actors working together.

These risks are organised, deliberate, and often repeated across different locations or operations.

Examples include organised cargo theft rings, smuggling networks operating through supply chains, insider collaboration, or coordinated fraud.

A single checklist will not stop a wolf pack. These threats require intelligence sharing, investigative capability, and coordination across departments or organisations.

They also require situational awareness beyond a single operational area.

THE HYDRA ADAPTIVE RISK

Hydra risks are the most frustrating type of threat because they evolve when attacked.

In Greek mythology, the Hydra was a multi-headed serpent that regenerated two heads for every one that was cut off. Hercules eventually realised that simply fighting the creature was not enough. He had to change the conditions that allowed it to regenerate.

Modern threats behave in much the same way.

Cybercrime networks, terrorist organisations, disinformation campaigns, and complex insider threat ecosystems all adapt to defensive measures. Shut down one pathway and another emerges.

Traditional incident response often treats each manifestation as a separate problem, but in reality these threats are part of a constantly evolving system.

Hydra risks cannot be defeated through static controls. They require adaptive governance systems capable of learning and responding continuously.

THE DRAGON SYSTEMIC RISK

Dragons represent systemic threats capable of destabilising entire organisations or industries.

These risks do not simply cause isolated incidents. They can reshape the environment in which organisations operate.

Examples include geopolitical conflict affecting air routes, major supply chain disruptions, technological shocks, or global economic instability.

These events sit beyond the scope of traditional security departments. They require strategic oversight, executive engagement, and resilience planning at the organisational level.

When a dragon appears, the question is no longer how to prevent an incident. The question becomes whether the organisation itself can adapt and survive.

THE PARASITE INTERNAL DECAY

The final creature is often the most dangerous because it develops inside the organisation itself.

Parasite risks are not external threats. They emerge from internal cultural conditions that gradually weaken an organisation's ability to recognise and respond to risk.

They appear when reporting is quietly discouraged, when uncomfortable information stops travelling upward, or when compliance processes become more about appearances than effectiveness.

Over time, these conditions erode situational awareness. Small problems go unreported. Warning signals are missed. Decisions are made based on incomplete or distorted information.

Unlike snakes, wolves, hydras, or dragons, parasite risks do not arrive suddenly. They develop slowly, often unnoticed, until the organisation's capacity to see emerging threats has already been compromised.

Many major organisational failures are not caused solely by external events, but by internal cultures that have stopped listening to themselves.

In that sense, parasites do not simply weaken an organisation. They create the conditions in which every other creature becomes more dangerous.

Recognising these different types of risk is the first step in understanding why traditional security approaches often struggle in complex environments.

Most systems are built to catch snakes.

Modern threats behave more like wolves, hydras, and dragons.

And sometimes the greatest danger is the parasite that slowly weakens the organisation from within.

WHEN THE CREATURES APPEAR IN THE REAL WORLD

Metaphors are useful, but the aviation industry has already encountered each of these "creatures" in practice.

THE SNAKE LOCAL OPERATIONAL FAILURES

Simple operational failures occur every day in aviation.

A gate left unsecured.

An expired access badge.

A baggage reconciliation error.

These are classic "snake" risks. They are localised, visible, and usually resolved through procedures, inspections, or corrective action.

Compliance systems are highly effective at identifying and removing these threats, which is why traditional aviation security frameworks have historically focused on this level of risk.

THE WOLF ORGANISED CRIMINAL ACTIVITY

More complex threats emerge when multiple actors coordinate their actions.

Cargo theft networks operating across airports are a good example. These groups exploit weak points in supply chains, insider access, and predictable operational patterns.

Stopping a wolf pack requires more than compliance. It requires intelligence sharing, investigative capability, and coordination between security teams, law enforcement, and operational departments.

Without that coordination, wolves can operate undetected for long periods.

THE DRAGON SYSTEM-LEVEL DISRUPTION

Dragons represent systemic risks capable of reshaping the environment in which organisations operate.

Unlike other threats, dragon events are not simply security incidents. They can alter the conditions under which entire industries function.

Geopolitical conflicts that close airspace, global pandemics that halt international travel, major supply chain disruptions, or technological shocks can all force organisations to rethink how they operate.

These events sit beyond the traditional boundaries of security departments. They involve complex interactions between political, economic, technological, and operational systems.

When a dragon appears, the challenge is no longer simply preventing an incident.

The challenge is whether the organisation itself can adapt and continue to function.

At this level, security becomes inseparable from governance, strategy, and organisational resilience.

THE HYDRA ADAPTIVE THREAT NETWORKS

Hydra risks are the most frustrating type of threat because they evolve when confronted.

Hydra risks appear when adversaries adapt to defensive measures. Aviation security has repeatedly experienced this dynamic: when one pathway is closed, experimentation quickly shifts to another.

Modern threats often behave in much the same way.

Cybercrime networks, terrorist organisations, disinformation campaigns, and complex insider threat ecosystems adapt quickly when defensive measures are introduced. Shut down one pathway, and another appears. Disrupt one network and activity shifts elsewhere.

In this sense, “Hydra risks” are not simply individual incidents but adaptive threat systems that evolve in response to the environment around them.

Traditional incident response tends to treat each manifestation as a separate problem. In reality, they are usually part of a broader pattern of behaviour.

Hydra risks cannot be managed through static controls alone. They require organisations to detect weak signals early, share intelligence widely, and adapt continuously.

These examples illustrate an important reality.

Aviation organisations encounter every level of the risk ecosystem. But the systems used to manage those risks are often designed primarily for snakes.

Security Management Systems provide a way to move beyond that narrow focus and build organisations capable of responding to the full spectrum of modern risk.

FROM SURVIVAL TO STRATEGY: THE ORGANISATIONAL SECURITY PYRAMID

Understanding the different "creatures" of risk explains why many security systems struggle in complex environments. But it also raises an important question.

Why do some organisations manage these risks effectively, while others remain constantly reactive?

The answer often lies not in the threats themselves, but in the **maturity of the organisation managing them**.

A useful way to understand this progression is to borrow a concept from psychology: **Maslow's hierarchy of needs**.

Maslow proposed that humans progress through stages of development, beginning with basic survival and eventually reaching self-actualisation.

Similar maturity models are frequently used in governance and risk management frameworks to describe how organisations evolve from reactive compliance toward integrated strategic resilience.

Organisations evolve in a remarkably similar way.

When applied to security and risk governance, this progression forms what we might call the **Organisational Security Pyramid**.

LEVEL 1:
OPERATIONAL SURVIVAL

At the base of the pyramid lies operational survival.

The organisation's primary goal at this stage is simply to remain compliant and operational.

Security activity focuses on access control, screening, physical protection, and regulatory adherence. The mindset is straightforward: stay legal, avoid fines, and maintain basic operational continuity.

Most security frameworks begin here, and many organisations never move far beyond it.

These environments are well-equipped to deal with **snakes**. Simple risks can be identified and removed through inspection and compliance monitoring.

But more complex threats often remain outside their field of vision.

LEVEL 2:
OPERATIONAL SAFETY

The next stage introduces more structure.

Here the organisation begins implementing formal risk assessments, procedures, reporting systems, and compliance monitoring mechanisms. Incidents are analysed and corrective actions are taken.

The mindset shifts slightly from simple compliance to **incident prevention**.

At this level, organisations can address both **snakes and some wolf-type risks**, particularly where coordinated activity becomes visible through repeated patterns.

However, the system still remains largely reactive. The organisation responds to problems after they emerge rather than anticipating them.

LEVEL 3:
ORGANISATIONAL TRUST

This is the level where security systems begin to transform.

Organisations at this stage invest heavily in **culture**.

Reporting becomes non-punitive. Leadership visibly supports transparency. Departments begin sharing information rather than operating in isolation.

Security stops being the responsibility of a single department and becomes a **shared organisational function**.

The mindset changes to something far more powerful:

"We protect this organisation together."

At this stage, coordinated threats such as **wolves** can be detected much earlier, and the organisation begins to recognise the early signals of **hydra-type risks**.

LEVEL 4:
PROFESSIONAL OWNERSHIP

When organisations reach this level, risk awareness becomes embedded across the workforce.

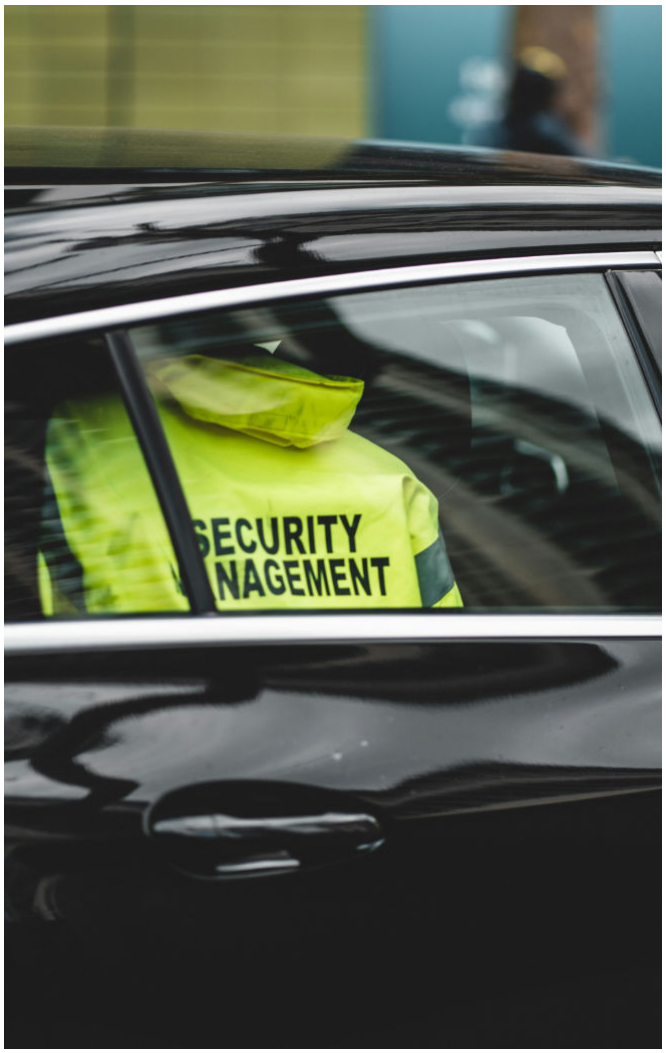
Frontline personnel actively identify emerging threats. Reporting becomes routine rather than exceptional. Performance indicators track risk signals and operational feedback loops drive continuous improvement.

The mindset shifts again.

“I am responsible for protecting this operation.”

Security systems at this level can begin managing **hydra risks** effectively because the organisation itself becomes adaptive.

Threats evolve, but the organisation evolves faster.



LEVEL 5:
STRATEGIC SECURITY

At the top of the pyramid, security becomes a strategic function.

Risk intelligence informs executive decisions. Governance structures integrate security, safety, operational, and strategic risk considerations. Leaders view resilience as a core component of organisational performance.

Security is no longer a cost centre. It becomes part of how the organisation protects revenue, reputation, and operational continuity.

It becomes a mechanism for protecting enterprise value, safeguarding reputation, and ensuring long-term organisational survival.

At this level, organisations can prepare for **dragons**.

They may not prevent systemic shocks, but they can recognise them early and respond with resilience.

Understanding where an organisation sits within this pyramid is critical.

Many companies assume they are operating at advanced levels of security maturity when in reality they remain firmly positioned within the lower tiers of compliance and incident response.

And when the environment becomes turbulent, the difference between these levels becomes painfully visible.

Organisations designed to catch snakes struggle when confronted with hydras.

Those that have developed true security maturity are better prepared to face dragons.

SEMS:
THE ORGANISATIONAL NERVOUS SYSTEM

If the “Five Creatures of Risk” help us understand the nature of modern threats, and the Organisational Security Pyramid explains how organisations mature in their response to them, then the question becomes clear.

What allows an organisation to move up the pyramid?

The answer increasingly lies in the adoption of **Security Management Systems** (SeMS).

SeMS was originally developed within aviation as a way to move security beyond purely reactive measures. The approach aligns with broader trends in risk governance that emphasise proactive management, cultural engagement, and continuous improvement. Instead of focusing solely on compliance and incident response, it encourages organisations to build systems capable of **learning, adapting, and continuously improvin**g.

At its core, SeMS introduces four essential capabilities.

First, it establishes structured mechanisms for **risk identification**. This includes reporting systems, monitoring processes, and the ability to capture weak signals before they escalate into incidents.

Second, it enables **information flow** across the organisation. Risk information is no longer trapped within a single department but becomes part of a wider intelligence picture shared across operational functions.

Third, it supports **adaptive decision-making**. By continuously analysing risk data, organisations can update procedures and responses in line with changing threat environments.

Finally, it strengthens **governance and accountability**, ensuring that leadership remains actively engaged in managing organisational risk.

Taken together, these capabilities create something much more powerful than a traditional security department.

They create an organisational **nervous system**.

Just as the nervous system allows the human body to sense danger, process information, and respond appropriately, a mature SeMS allows an organisation to detect threats early, understand their implications, and adapt before damage occurs.

This capability becomes particularly important when dealing with hydra and dragon risks.

These threats cannot be eliminated through static controls alone. They require organisations to maintain constant awareness, share intelligence rapidly, and adapt continuously.

SeMS provides the framework through which that adaptation can occur.

THE PERSONAL SECURITY CONNECTION

One of the most powerful shifts that occurs as organisations move up the security maturity pyramid is a change in how individuals perceive their role in managing risk.

At lower levels of maturity, security is seen as the responsibility of a specific department. Employees follow procedures but rarely feel personally connected to the broader security posture of the organisation.

As culture develops, this perception begins to change.

Individuals start to recognise a simple but important connection:

- Organisational security protects operational stability
- Operational stability protects jobs.
- Jobs protect personal financial security and family wellbeing.

In other words, organisational security becomes **personal security**.

When this connection is understood, behaviour changes.

Employees begin to report concerns earlier. Situational awareness improves. Teams actively protect the systems they rely on for their own livelihoods.

The organisation becomes self-correcting.

This cultural shift is one of the most important outcomes of an effective SeMS. It transforms security from something imposed externally into something **owned collectively** by the workforce.

FROM COMPLIANCE TO RESILIENCE

Modern organisations operate in environments where risks evolve rapidly and often unpredictably.

Compliance-based security systems remain necessary. They provide the foundation for controlling simple risks and maintaining regulatory standards.

But compliance alone is no longer sufficient.

To navigate the complex threat environments represented by wolves, hydras, and dragons, organisations must develop systems capable of sensing, learning, and adapting.

Security Management Systems provide a pathway for making that transition.

They move security beyond the narrow confines of enforcement and compliance and place it within the broader context of governance, resilience, and organisational survival.

Ultimately, the question facing leaders is not simply whether their organisation is compliant.

It is whether their organisation is capable of recognising and responding to the full spectrum of modern risk.

Because while most security systems are designed to catch snakes, the world today contains far more wolves, hydras, and dragons than many organisations realise.

THE LEADERSHIP QUESTION

Security environments do not stand still. They evolve.

Simple operational failures will always exist. Snakes will continue to appear somewhere in the system. But modern organisations must now contend with far more complex threats.

- Coordinated criminal networks operate like wolf packs
- Adaptive adversaries behave like hydras
- Systemic shocks can emerge like dragons

And in many organisations, the most dangerous vulnerability is the parasite that quietly erodes culture from within.

The uncomfortable reality is that many security systems are still designed for a world that contained mostly snakes.

That world no longer exists.

Security Management Systems offer something different. They create the structures through which organisations can sense emerging risk, share intelligence, and adapt before small problems become strategic failures.

In doing so, SeMS transforms security from a compliance exercise into something far more important: a mechanism for organisational resilience.

Which leaves leaders with a simple but uncomfortable question. **Are you building security systems to catch snakes… or preparing your organisation to face dragons?**

ISRM

ABOUT

THE INSTITUTE OF STRATEGIC RISK MANAGEMENT

The Institute of Strategic Risk Management (ISRM) is a leading global centre for the promotion and sharing of best-practice strategic risk and crisis management capabilities and thought leadership amongst practitioners, academics and policy makers. Across the Institute's global chapter network, our Members and Fellows help progress and promote the underlying understanding and capabilities associated with strategic risk and crisis management, alongside developing their own personal and professional networks.

The ISRM provides best-practice training, hosts leading events across its global and local networks, and provides strategic advice to support organisations' management of complex risks.

www.theisrm.org

info@theisrm.org