ISRM

Bidvest NOONAN

Rethinking Risk Management

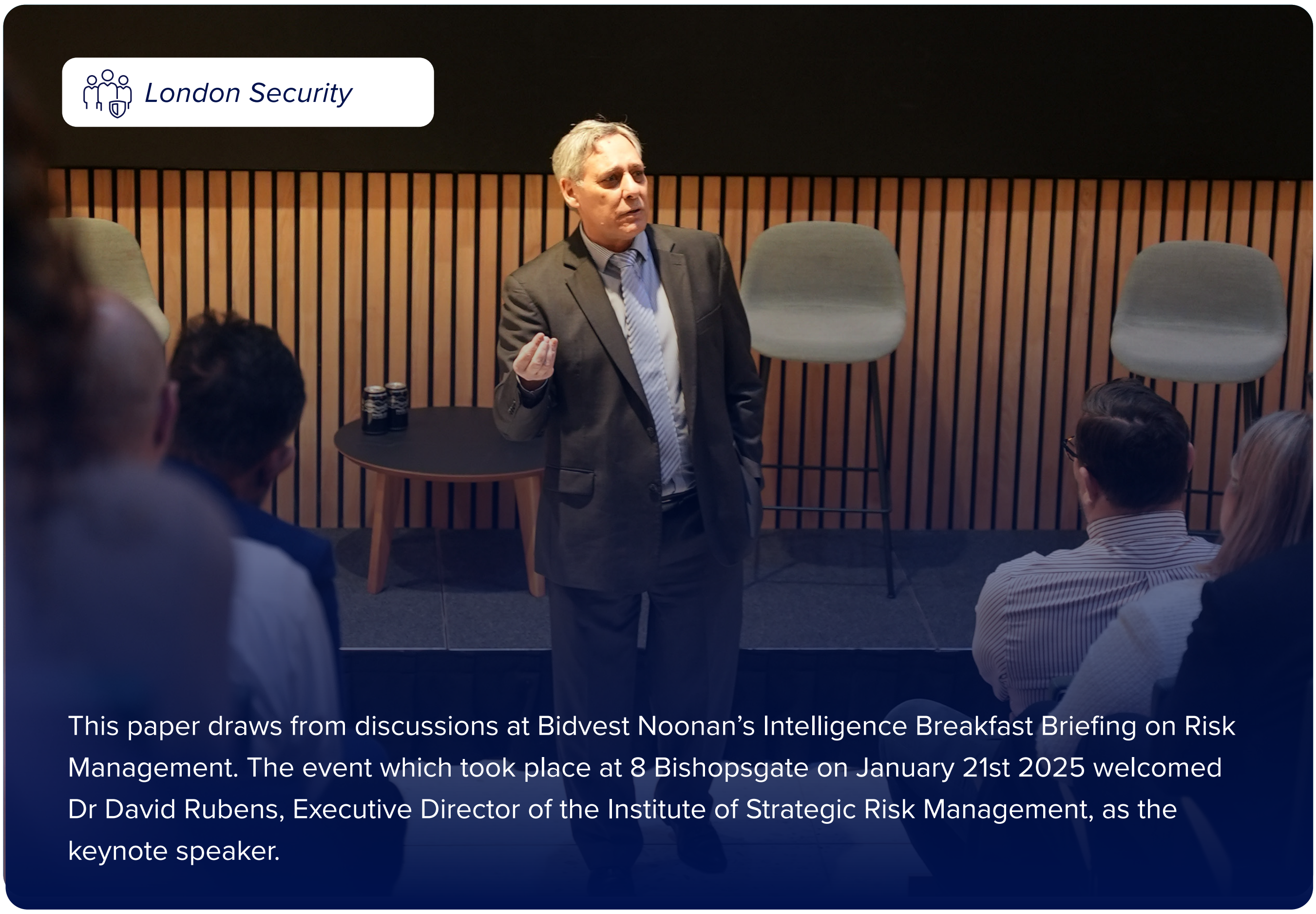
Managing risk in the era of permacrisis

Executive Summary

The risks businesses face today are changing. Threats are no longer simple or predictable. Extreme weather is happening in unexpected places. Cybercrime is mixing with physical security risks. Public disorder is becoming harder to manage. The threat of terrorism remains a concern, with risks evolving beyond traditional attacks to include cyberterrorism and infrastructure disruption. These problems are not one-off events. They are part of a growing permacrisis where risks overlap, escalate and create ongoing challenges.

Many organisations still rely on old ways of assessing risk, assuming that threats are separate and manageable. But recent events have shown that risks can combine, spread and cause serious disruption. What worked in the past may not work in the future.

This white paper looks at five key factors that affect modern risk management. Location, time, scale, impact and recovery time. It explains why these factors matter and how businesses can prepare for the unexpected. Read on to understand the risks ahead and learn what businesses can do to stay protected in an era of permacrisis.



London Security

This paper draws from discussions at Bidvest Noonan's Intelligence Breakfast Briefing on Risk Management. The event which took place at 8 Bishopsgate on January 21st 2025 welcomed Dr David Rubens, Executive Director of the Institute of Strategic Risk Management, as the keynote speaker.

The Evolution of Risk Management

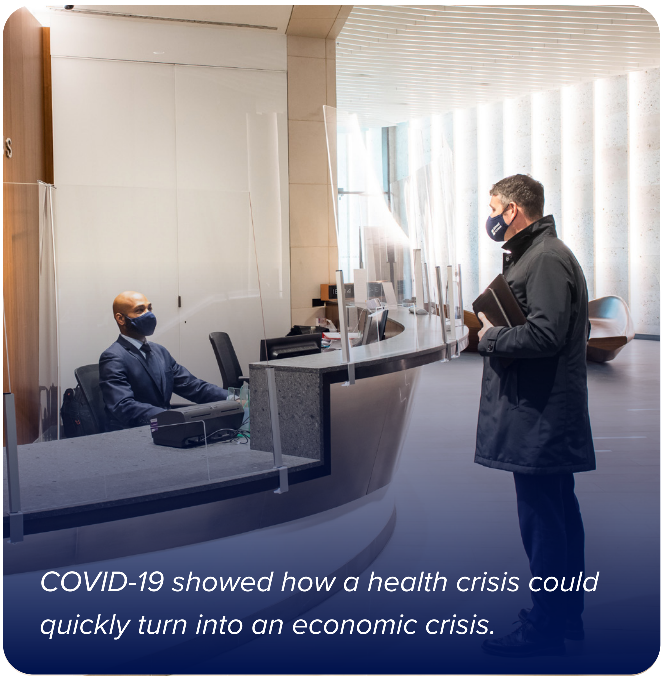
Risk management has changed a lot over the years. In the past, companies assumed risks could be predicted and controlled using set methods. The thinking was that if something had happened before, it could be measured and planned for in the future. This worked well in a world that was stable and changed slowly. However, today's world is much more unpredictable. Problems in one place can spread quickly and affect businesses everywhere.

A financial crisis in one country can lead to job losses in another. Extreme weather events, such as floods and storms, are happening more often and causing major damage.

> *The terrorist attacks of September 11, 2001 changed the way people think about risk forever.*

Technology has also created new risks. Cybercriminals can steal important information or disrupt entire systems with a single attack. Companies must now think about how to protect themselves from threats that didn't exist just years ago. The terrorist attacks of September 11, 2001 changed the way people think about risk forever. Before this, most organisations focused mainly on financial risks and operational risks. However, 9/11 showed how unexpected events could have the most devastating impact. After the attacks, businesses and governments realised they needed to prepare for threats that seemed unlikely but could still happen.

A more recent example is the COVID-19 pandemic. It showed how a health crisis could quickly turn into an economic crisis. Supply chains broke down, businesses shut their doors, and millions of people lost their jobs. Many companies had no plan for a global pandemic and struggled to survive. Those that had flexible plans in place were able to adapt more quickly. The main challenge for businesses today is being able to handle unexpected problems when they arise. It's impossible to predict every risk, so the focus should be on building systems that can adapt to new challenges. Companies that are prepared to adjust their strategies quickly and respond to disruptions will be more successful in the long run.



COVID-19 showed how a health crisis could quickly turn into an economic crisis.

Risks

Security professionals deal with a very wide range of risks every day. The following risks arethe focus of many security professions:

Workplace violence and active assailants

Security teams need to be prepared for aggressive behaviour and violence including armed attacks. Thorough training, clear protocols, strong awareness, and quick responses are needed to help keep people safe.

Terrorism and organised crime

Terrorism and organised crime pose risks to everyone but especially those in high-profile locations, corporate offices, and public spaces. Security teams play a very important role in preventing incidents through careful monitoring, robust access control, and by identifying suspicious behaviour such as hostile reconnaissance. Close collaboration with law enforcement and intelligence agencies strengthens threat detection and response.

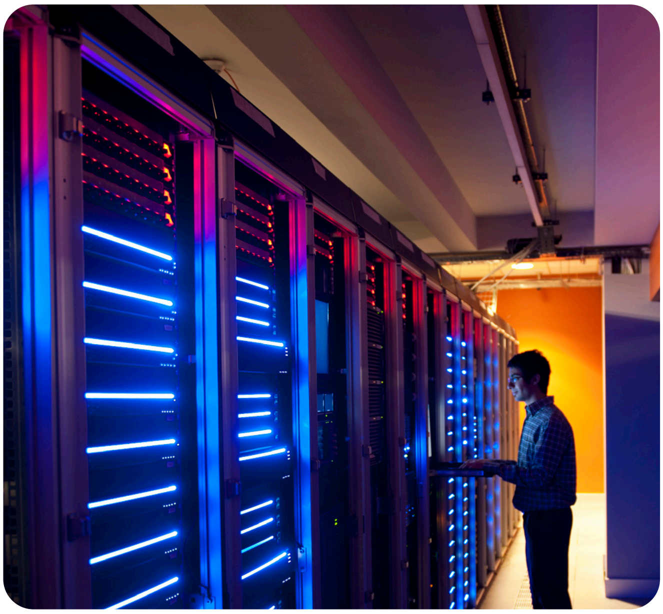
The current threat level for terrorism in the UK is substantial, meaning an attack is likely.

Cybersecurity Threats

Cybersecurity attacks are often associated data breaches and ransomware however they can also affect physical security for example compromising access control systems, CCTV networks, and security technology. Strong protections and regular monitoring reduce the risk.

Insider threats

Insider threats come from employees or contractors who misuse their access to restricted areas or sensitive information. Strict access control, background checks, and monitoring can help reduce this risk.



According to the Cyber Security Breaches Survey 2024, 50% of businesses reported experiencing some form of cyber attack in the past 12 months.

Heavy rain led to rivers in Yorkshire bursting their banks in 2020 causing significant damage. Severe flooding is becoming increasingly common in the UK.

Severe weather and environmental risks

Severe weather events such as flooding and storms, can disrupt security business operations. Security teams must help to mitigate the impact of these events through planning however they must plan for evacuations, asset protection, and site safety during extreme conditions.

Regulatory and compliance risks

Security teams need to stay informed about changing laws, data protection rules, and industry standards to protect themselves and their clients from penalties and maintain compliance. By recognising these risks, security professionals can take practical steps to enhance safety, reduce threats, and maintain strong security operations.

Five Key Factors to Understand Risks

Dr David Rubens, Executive Director at the ISRM outlined five key factors that influence risk management decisions: location, time, scale, impact, and recovery time. Each one plays a role in shaping how we prepare for and respond to threats.

Location – Where Does It Happen?

Some risks are tied to specific places, such as earthquakes in fault zones or flooding in low-lying areas. But the world is changing. Extreme weather is appearing in unexpected regions, cyberattacks affect businesses worldwide, and local conflicts disrupt global supply chains. Risks no longer stay in one place. For businesses, this means risk assessments must be reviewed regularly. Just because something has not happened in a particular location before does not mean it will not in the future.

Time – When Does It Happen?

Many risks used to be seasonal or predictable. Wildfires had a season, and flu outbreaks came in winter. But patterns are shifting. Some threats, such as cybercrime, now operate continuously. Others, such as extreme weather, no longer follow their usual cycles.This makes preparedness more important than ever. Organisations need to move beyond just planning for predictable events and build resilience for year-round, unpredictable threats.

Scale – How Big Is It?

A minor incident affecting one part of a business can usually be contained. But what happens when multiple things go wrong at once? More risks are now overlapping. Businesses need to think beyond individual threats and consider how different risks interact. A strong risk management strategy looks at cascading failures and ensures that contingency plans cover multiple, simultaneous disruptions.

Impact – How Bad Is It?

Not all risks cause the same level of damage. Some are inconveniences, while others can shut down operations or even threaten lives. The challenge today is that the impact of risks is growing. A single ransomware attack can cripple an entire company, and a flood in one part of the world can disrupt businesses thousands of miles away. To manage this, organisations need to prioritise risks based on potential consequences, not just likelihood.

Recovery Time – How Long Until Things Return to Normal?

In the past, businesses expected to bounce back quickly after an incident. But now, some disruptions last for months or years. COVID-19 changed the way we work. Cyber breaches continue to affect companies long after systems are restored. Climate disasters are leaving some areas permanently uninhabitable. This means that risk management is about long-term adaptation. Companies that plan for extended recovery, invest in flexible systems, and build resilience will be in a far stronger position than those that assume they can return to business as usual quickly.

Leadership in Risk Management

Effective risk management leadership is about setting a vision, making tough decisions under pressure, and creating an adaptive and intelligence-focused culture. The best security leaders anticipate threats before they materialise, ensuring their organisations stay ahead of emerging risks.

Permacrisis

Security leaders are dealing with an environment of permacrisis, where new threats continuously emerge while existing ones persist. Leaders must manage multiple overlapping risks simultaneously, ranging from cyber threats to workplace violence, rather than dealing with one crisis at a time. In this state of Permacrisis the right risk management approach will incorporate reactive and proactive strategies.

Security Leadership and Influence

Despite their critical role, many security leaders struggle to gain strategic influence at the board level. Security is often perceived as a tactical function rather than a driver of business resilience. To shift this perception, security leaders must build strong cross-functional relationships, articulate the strategic value of security, and align risk management with broader business objectives.

The Challenge of Agility

We have all seen how quickly new security threats can emerge. In these moments security teams have to make decisions quickly and sometimes under immense pressure. Leaders need to ensure their teams have the tools and agility to respond well in these situations. Leaders can create frameworks that allow their security teams to be decisive, empowering them to make good decisions rather than waiting for top-down instructions in critical moments.

Smarter Decision-Making

The volume of data available to security leaders today is unprecedented, but it is only useful if leaders extract meaningful insights from it. The best security teams analyse data to detect patterns, identifying risks before they escalate. Data should inform everything from real-time threat responses to long-term strategic planning, ensuring that risk mitigation efforts are evidence-based.

The Importance of Stress-Testing and Scenario Planning:
The most resilient security teams rigorously test their readiness threats. Leaders arrange regular crisis simulations. These simulations put their teams through high-pressure scenarios, helping to identify weaknesses and refine their responses. This approach ensures that when real threats occur, security teams are well practiced in how to respond.

The Role of Technology in Risk Management

Technology plays a very important role in modern risk management, helping security teams spot threats early, respond quickly, and make informed decisions. With risks becoming more complex and linked, digital tools are increasingly invaluable.

Improving Risk Visibility and Decision-Making

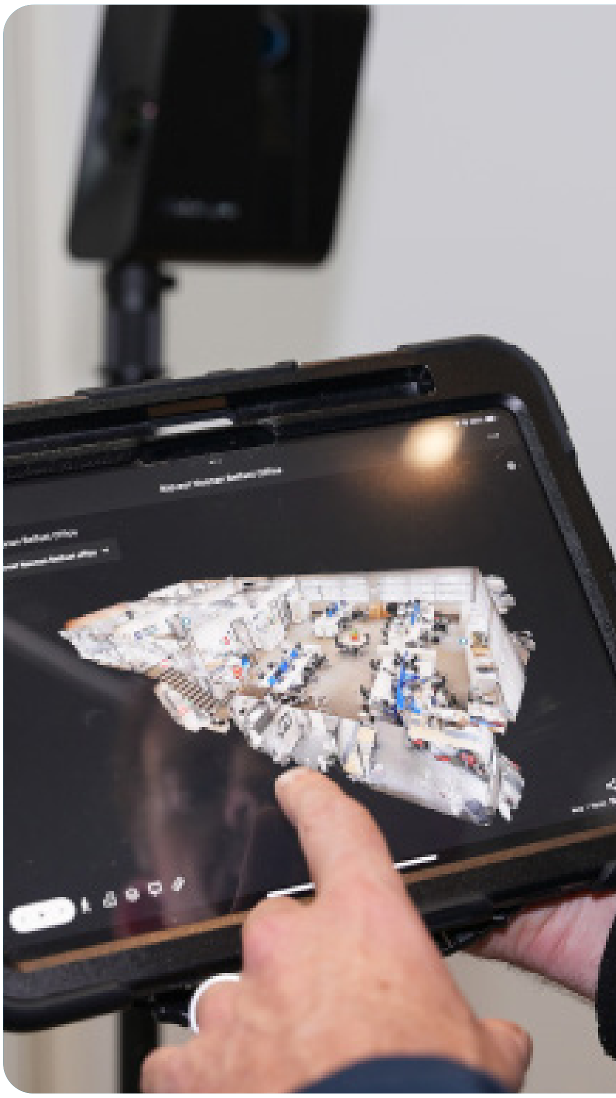
Risk management systems help monitor and track different types of security risks such as cyber threats, physical incidents, and operational disruptions into a single, clear view. This makes it easier for leaders to see potential risks, understand their impact, and take action before issues grow. Automated alerts and real-time reports also ensure that important information reaches the right people without delay.

The Move to Digital Occurrence Logs

Traditional paper-based occurence logs are being replaced by digital systems. By using digital occurrence logs, teams can:

- Capture and store detailed records of security incidents, including multimedia files.
- Analyse patterns and trends to identify repeated risks and prevent future issues.
- Ensure compliance with security policies and legal requirements by keeping accurate and accessible records.

These systems also link with other technologies such as digital operations platforms, creating a more complete picture of FM operations.

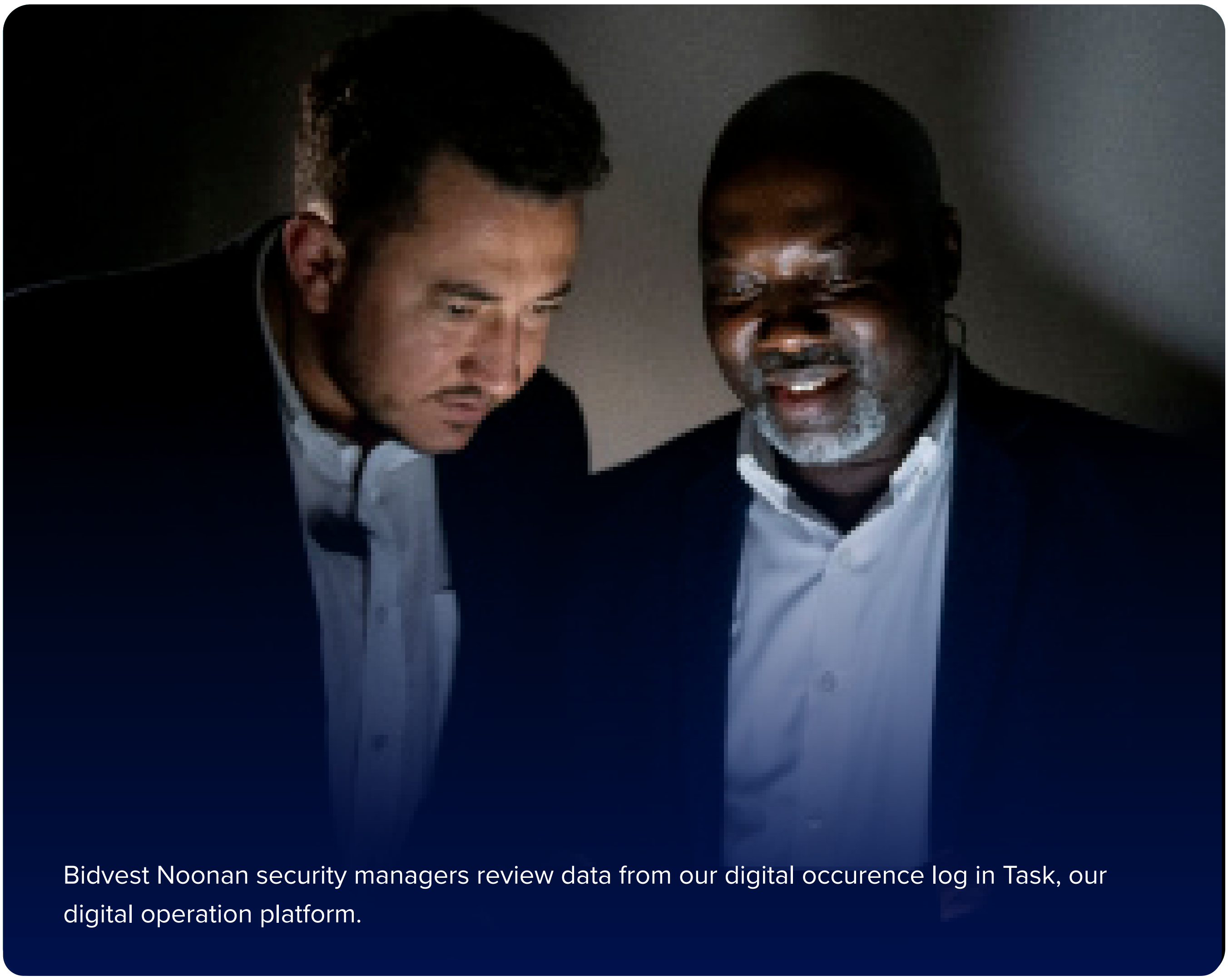


Intelligence and Early Warning Systems

Security teams use intelligence platforms to identify potential threats ranging from severe weather risks to protest action. These systems gather information from diverse sources such as news, government alerts, internal reports, and environmental monitoring systems.

By using intelligence tools, organisations can:

- Receive early warnings about risks that could affect their operations.
- Track developments in real time, ensuring that decision-makers stay informed.
- Plan responses effectively, reducing disruption and lowering the impact of incidents.



Bidvest Noonan security managers review data from our digital occurence log in Task, our digital operation platform.

The Human Factor

People play a central role in effective risk management. While technology and processes support risk reduction, it is individuals who assess threats, make decisions, and implement security measures. Well-trained and engaged employees are a company's first line of defence against risks.

Training and Awareness

Ensuring that employees understand risks and their role in mitigating them is essential. Regular training on security protocols, compliance requirements, and situational awareness helps create a proactive risk culture. Well-informed teams are more likely to identify and respond to threats effectively.

A Whole-Organisation Approach to Risk Management

Risk management is strongest when it is embedded across the entire organisation. Security is not just the responsibility of dedicated teams but requires collaboration across departments, including operations, HR, IT, and legal. A siloed approach weakens security effectiveness, while shared accountability strengthens resilience. Encouraging open communication about Risk Management helps identify vulnerabilities early and improve risk strategies.

The Importance of Recognition

When employees feel valued and understand their impact on security, they are more likely to support risk management. Recognising their contributions to risk management encourages proactive behaviour and reinforce good security practices. By prioritising people in risk management strategies, organisations can build a culture where security is everyone's responsibility.

Bidvest NOONAN

bidvestnoonan.com