ASSESSING RISK, REALISING OPPORTUNITY AND TAKING REWARD

Examining the techniques available to risk and security professionals

THREAT MONITORING

airmic

Control Risks

Foreword

In the five decades through which Control Risks has supported clients across the globe the political, technological, environmental and societal landscape has changed to a degree that few could have predicted. While this has undoubtedly created opportunities and wealth, and with it the attendant benefits, it has also been a catalyst for uncertainty, instability and conflict, and has under-lined the problematic nature of understanding and sense-making in this changing world.

Against this backdrop Control Risks embarked upon a research programme with our partners at Airmic. Our aim was to gain a better understanding of how organisations view the world today, and the means by which they attempt to monitor, map and comprehend a highly complex threat and risk environment. We wanted to identify how technology can be harnessed, and how this can provide insight to support decision-making and ultimately the realisation of opportunity.

We would like to thank our clients who kindly agreed to participate in the research and to Longitude for its expert assistance. We found the process both fascinating and enlightening. We hope in turn that this report will be of value to all those with an interest in the nature of the changing world and how threats can be better monitored and evaluated to enhance understanding and decision making.

Mark Whyte
Senior Partner, Control Risks

Inside...

About this research

This study is part of a wider research project discussing the future of the risk and insurance management professions, entitled, *Risk Management: Vision 2020.*

While the main report summarises the full findings of the research project, this is one of five deep dives into the core themes within *Risk Management: Vision 2020.*

The five reports are:

Assessing risk, realising opportunity and taking reward. Examining the techniques available to risk and security professionals.

Understanding external threats to an organisation. An analysis of the interconnected nature of geopolitical risks and how they can be managed.

The value of boardroom engagement. Aligning the organisation's risk profile with governance and liability awareness among directors and officers.

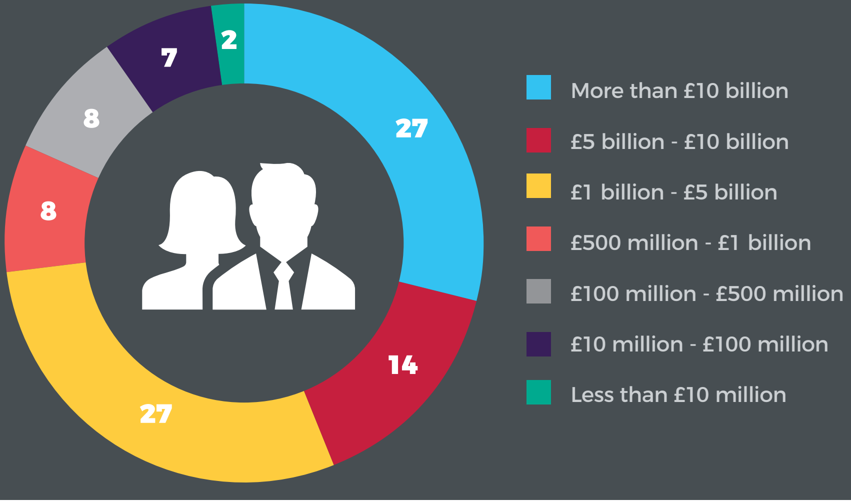
Turning data into information. Assessing the current and future role of data analytics in managing risk and insurance.

Transforming insurance for tomorrow's risks. Encouraging collaboration between customer, broker and insurer to move risk forward.

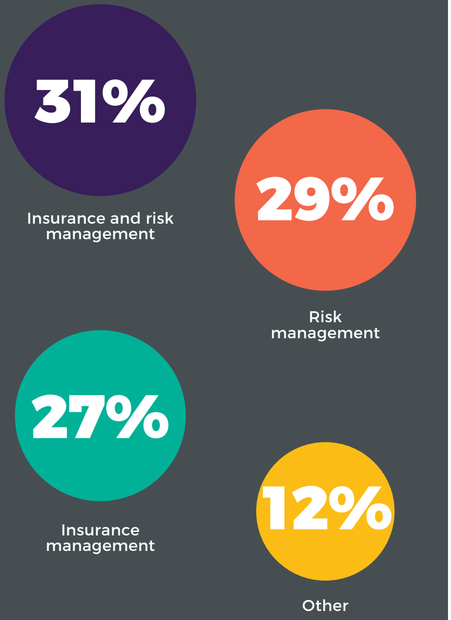
About the respondents

This report, produced by Airmic in collaboration with Longitude, is based on the responses of 157 members. While job roles and sizes of organisations vary, respondents primarily come from risk and insurance management and enterprise risk management at large multinational businesses. Due to rounding, and the use of multiple-choice questions, some figures and charts in this report may not add up to 100%.

Global turnover



Job role



Executive Summary

The threats facing organisations in 2019 are complex and increasingly intangible. With reputation and trust high on the mind of business leaders, softening the impact and preventing events from happening at all is more important than ever. Fire or flood damage to a factory may delay or halt production and result in substantial costs, but a cyber-attack that compromises the data of customers can have a long-term effect on trust and future engagement.

Risk professionals will be familiar with fire and flood mitigation techniques, but contributing to a monitoring and defence system that combats cyber-attacks will require collaboration with their colleagues across security, information technology, strategic intelligence and operations.

Similarly, unless the activities and developments within the local and geopolitical environment are monitored effectively risk professionals will be left unaware of the evolving political threats that risk disruption to their business and unable to plan accordingly.

Effective threat monitoring will put risk and security professionals on the front foot and bring them closer to senior strategic decision makers. In a fast-paced world, more sophisticated techniques and internal processes are required, demanding greater collaboration across the organisation. Implementing and leading threat monitoring activities can provide a platform for risk professionals to take centre stage within their organisation, add commercial and competitive value and identify new opportunities.

Risk professionals will need to work across their organisation's business units and functions to identify and prioritise the key threats, and work on an effective response to track their development and evolution.

This report, produced in partnership with Control Risks, highlights practical uses for threat monitoring and the relevant steps organisations should consider when embarking on this journey.

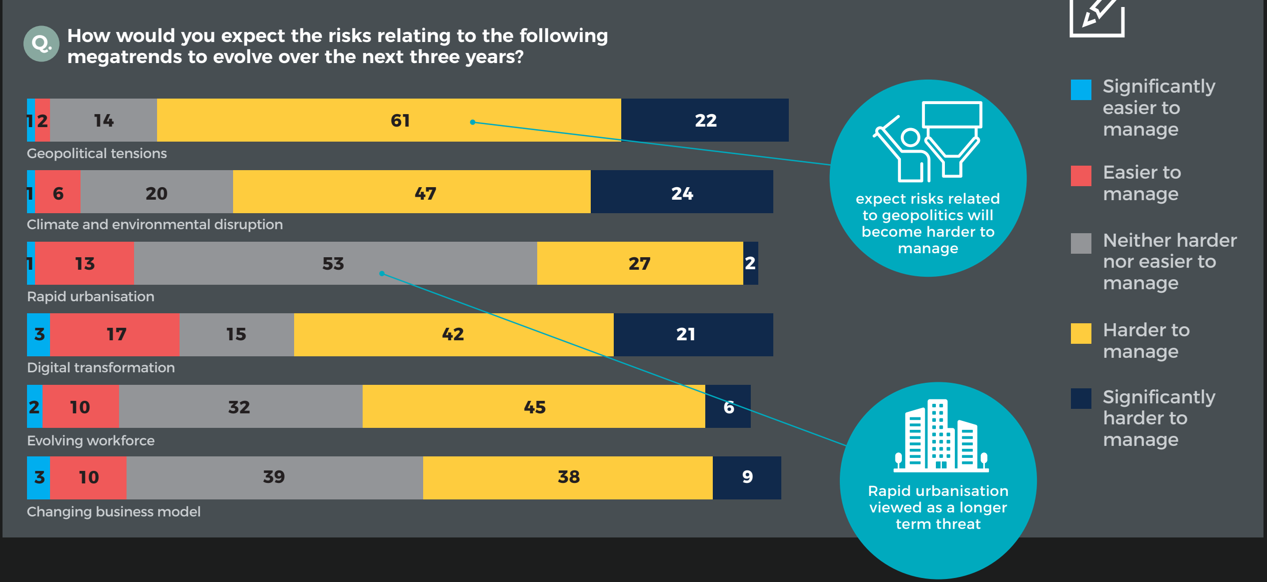
> The threats facing organisations in 2019 are complex and increasingly intangible

The priorities

As external factors top the list of concerns among risk managers, threat monitoring is becoming increasingly important. These threats are expected to only become harder to manage over the next three years with the risks associated with geopolitical tensions and climate and environmental disruption leading the way (Figure 1).

Results

Figure 1: Geopolitics and climate disruption present the biggest challenge



expect risks related to geopolitics will become harder to manage

Rapid urbanisation viewed as a longer term threat

These results match up with Control Risks' 2019 RiskMap outlook, where the US-China trade rift, American political deadlock and extreme weather disruption are among the top five risks.

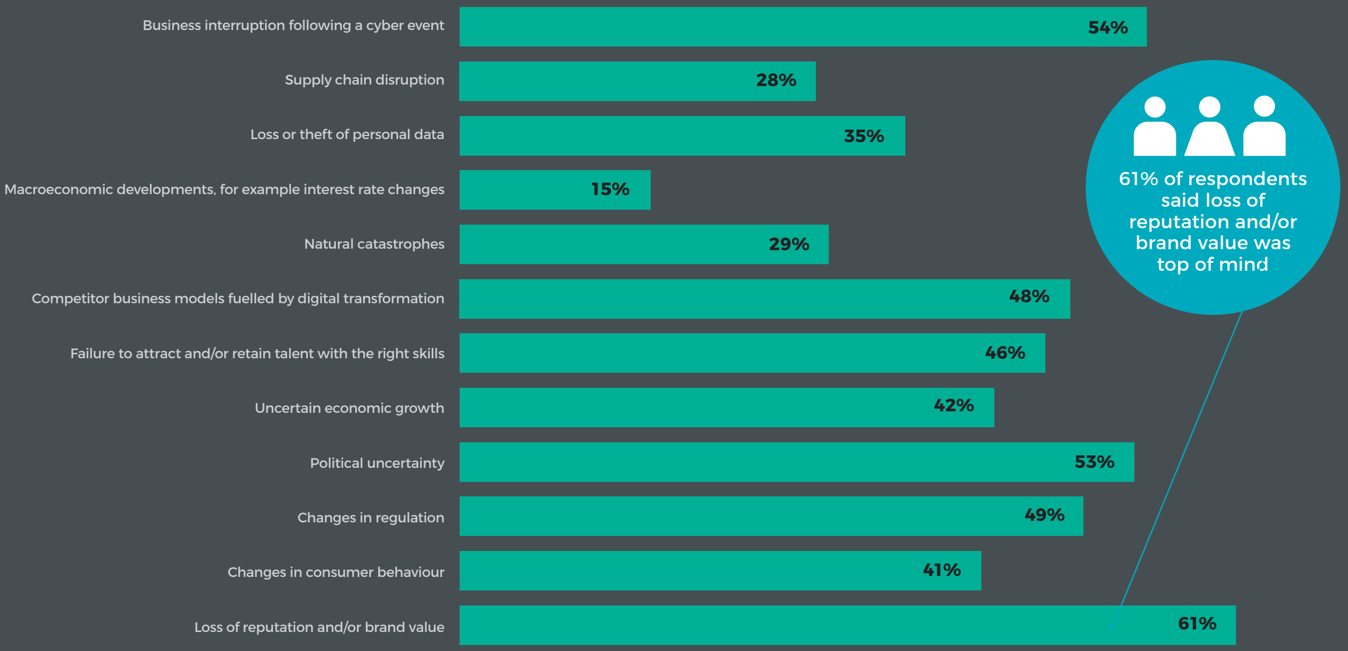
The global footprint of multinational corporations is naturally increasing exposure to the vagaries of geopolitics – from trade wars to real conflict. But recently, the degree of political risk faced by companies has intensified. A generation of business leaders conditioned by globalisation finds itself on the sharp edge of fierce national competition for jobs, technology and tax revenue. Business leaders are having to quickly recalibrate. Locating a new factory or attending an international summit is now a political statement as much as a commercial and operational consideration. In a fractured world order, the business of business is no longer just business.

Equally, it comes as no surprise that 71% of respondents expect risks associated with climate and environmental disruption to become "harder" or "significantly harder" to manage over the next three years. Some of 2019's worst business disruptions will not come from terrorist attacks but from extreme weather and its consequences. From storms and floods to droughts and forest fires, the costs of interrupted production, distribution, sales and travel will skyrocket in 2019. Last year's record for weather-related insurance claims will likely be surpassed. Extreme weather and all it brings have never been more significant as a business risk.

When asked to choose their top three business risks over the next three years (Figure 2), business interruption following a cyber event was identified second (behind loss of reputation and/or brand value), while loss or theft of personal data is also on the radar. Organisations that operate across more than one of Europe, America and China find themselves having to navigate vastly different cyber and data security environments, as highlighted by this risk's place at number two in the RiskMap. As a result, monitoring the activities of data regulators and ensuring cyber defences are robust and up to date are becoming increasingly important.

Figure 2: Reputation, cyber and political uncertainty lead concerns

Q. Of the following, please rank the top five front-of-mind business risks that you would expect in three years' time?



61% of respondents said loss of reputation and/or brand value was top of mind

> “Monitoring the activities of data regulators and ensuring cyber defences are robust is becoming increasingly important

The response

Only a third of respondents, however, believe that threat monitoring has been integrated and is valued by all relevant parts of their organisation (Figure 3). Even in cases where the risk manager is aware of threat-monitoring tools being used sporadically across their organisation it is unlikely to be as effective as taking a holistic approach.

Before designing and implementing an effective threat-monitoring programme, the organisation needs to understand what it is monitoring against. Such an assessment will encompass a broad array of areas and should bring together all individuals who are concerned with threats across the organisation. They will include security managers, government affairs teams, public relations teams and risk professionals.

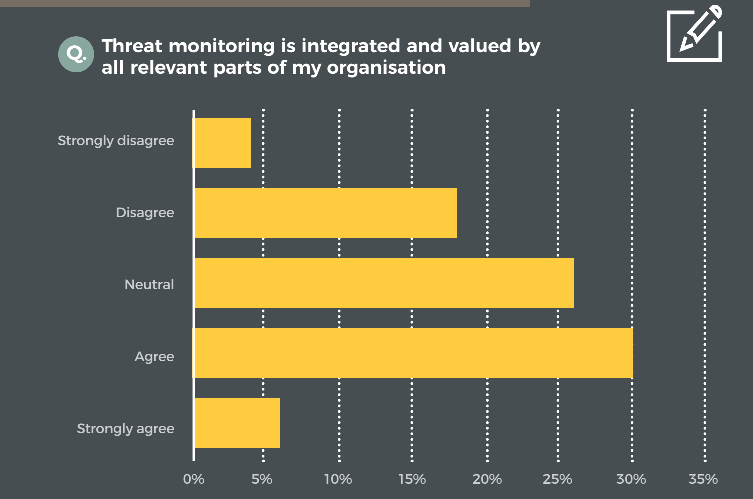
"The maturity of threat monitoring programmes depends on the ability to pull different parts of the organisation together to create a holistic view of threats," says Oliver Wack, partner at Control Risks.

Five key questions to ask internally:

- Where do we operate and what is our footprint?
- What third party relationships do we have?
- Where does our key revenue come from?
- What regulatory and government actions / changes are we exposed to?
- What activist groups or individuals may seek to disrupt our business?

>

Figure 3: The value of threat monitoring is not fully realised



> **Organisations need to understand what they are monitoring against**

> In only the rarest of cases will an organisation have the capacity or resources to monitor all potential threats. As such, it must prioritise the key threats and identify what qualitative and quantitative information can be tracked, collected and analysed in relation to these. The threat assessment should also identify the key triggers that will indicate an incident is about to happen or has already begun.

While multinational businesses are increasingly building global security operations centres (GSOCs) and employing teams of analysts to identify and monitor a multitude of threats, others have found working with third parties an effective solution. This approach can range from contracting a team of analysts who are focused on one particular area, to putting in place a 'virtual GSOC' where they pay for one half or one quarter of an analyst that contributes to broader information collection.

Threat monitoring in practice: cyber

While cyber may primarily be viewed as a risk that needs to be tracked, analysed and guarded against online, different levels of cyber threat monitoring will involve different parts of the business and different tools. Below are four approaches to cyber threat monitoring that combine quantatitve and qualitative sources.

1. Technical threat monitoring and intelligence –
Understand and analyse the immediate threats to your organisation detected from the inside and the outside.

In the past 10 years, organisations, starting with the financial services sector, have embraced technical threat monitoring systems. These systems monitor activity across the network and determine whether threats are present by correlating events with known malicious behaviour from other networks. They detect activity that is happening today and can identify a cyber attack, but they **struggle to predict what might happen tomorrow**. This technical approach is critical to keep the lights on, but the speed at which bad actors can change tactics and alter their indicators makes their activities harder to anticipate.

2. Operational threat monitoring and intelligence – Intelligence on inbound threats to your organisation, before they hit your network

With the growth of online platforms where threat actors from around the world communicate, plan and prepare their operations, the importance of monitoring external sources has increased significantly. Operational threat monitoring is used by a growing number of organisations to understand the intent of online groups to target them. Sources such as social media, instant messaging platforms and online forums and blogs provide defenders with the ability to analyse the chatter of threat actors and plan their defences accordingly.

However, the volume of data and the challenge of analysing information accurately is important. Many organisations struggle with driving actionable intelligence from chatter and can drown in a huge volume of information. Applying intelligence tradecraft to the collection and analysis of operational information can help in anticipating short-term operations against the organisation.

“

Multinational businesses are increasingly building global security operations centres (GSOCs)

> **3. Tactical threat intelligence –**
Actionable intelligence analysing the tactics, techniques and procedures of cyber threat actors targeting organisations across the world.

Monitoring and understanding the tactics being used by potential cyber attackers is an effective way to get ahead of the threat. One area to monitor is intelligence sharing platforms and cross-industry sharing initiatives – for example, a threat group wanting to attack a particular organisation has often carried out similar operations against others. Analysis of the modus operandi of threat actors impacting a sector, or a region, can be highly beneficial to help inform defensive strategy. This information is beginning to be monitored effectively by organisations and can also be sourced directly from a range of providers.

The challenge, however, is that with so many bad actors out there, it is sometimes difficult to clearly understand which ones are likely to pose a threat to the organisation. This requires a deeper, more strategic understanding of the threat landscape.

4. Strategic threat intelligence –
Forward looking intelligence helps organisations understand global developments and trends in the cyber threat landscape. This informs cyber security strategy and enables them to understand how cyber security threats can be contextualised within the broader threat landscape.

The fourth tier is a relatively new approach and remains less common among commercial organsiations today. It encourages the organisation to ask what makes it an attractive target to any actors. These may be rogue individual attackers, organised crime members, hacktivists or nation states. Asking this question should inform the approach to the operational and tactical levels and feed into the organisation's behaviour and strategy more broadly.

If the organisation is considering entering a new market, then strategic threat intelligence will help it understand how the cyber threats are different and may require a different approach to levels one and two. For example, it may be responding to a government tender in an African country that has no prior experience of doing business in. In that instance, strategic threat intelligence may be able to assess the risk of being spied on during the bid process.

Source: Control Risks

Analysis of the modus operandi can be highly beneficial to help inform defensive strategy

The maturity of the above approach to cyber threats varies across organisations, but it is becoming rare for them not to be implementing any of these tactics. The financial services sector is generally leading the way on cyber defence systems and threat monitoring because it has been the most targeted, while companies in the oil and gas sector are already embracing the strategic threat monitoring and intelligence analysis approach.

Cyber threat monitoring has become increasingly pervasive in the commercial sector. Organisations have invested in in-house technology, developed skills and purchased commercial sources of data in order to enhance their awareness of the cyber threats they face. Similar principles can be applied to a much broader range of risks and threats from security to regulatory ones.

FINANCIAL SERVICES TARGETED

In February, the Financial Conduct Authority reported that financial institutions suffered a five-fold increase in the number of cyber attacks on their systems last year. In 2018 there were 145 reported breaches, with retail banks seeing the largest percentage increase in threats. The sudden increase may be a result of the introduction of GDPR in May 2018 which requires the reporting of a cyber attack within 72 hours.

Role of technology

The majority of respondents recognise that new technologies can enhance their approach to threat monitoring (Figure 4), while almost half say their organisation is already investing in new technologies to enhance their understanding of the dynamics in their environment and deliver greater visibility (Figure 5).

Members are right that new technology has produced more effective tools that can be deployed as part of threat monitoring systems. These can come in the form of sophisticated platforms that leverage algorithms for collection and analysis of relevant data points, that can be utilised to data mine and identify trends within the threats that are being monitored.

Providers such as DataMinr, Threatminder and Banjo can provide tools that aggregate and interpret social media feeds, and provide easy and intuitive search functions and dashboards to interpret the information. Another heavy focus for tools is in the cyber threat realm, with a host of products such as LookingGlass, FireEye, CrowdStrike and offerings available in this space.

But there appears to be limited competitive offerings in the space of bridging the gap between incident monitoring and assessments and business planning around security, political and other risk management postures. Users should be aware, however, that such tools are most effective when they are utilised alongside human interaction and input.

Organisations can easily invest a lot of time and resources buying in new technologies that collect large volumes of data, but unless there are individuals assessing the relevance of output indicating, for example, that an event

"

The human touch will refine and improve return on investment

is taking place nearby, an effective and timely response may be hard to action.

While the human touch will refine and improve return on investment, one approach quickly gaining traction and minimising the human input is Security Orchestration, Automation and Response (SOAR). This approach integrates multiple software programs in an effort to automate response to low-level security threats.

>

Figure 4: Risk professionals are embracing the role of technology

Q. New technologies can enhance a proactive approach to threat monitoring

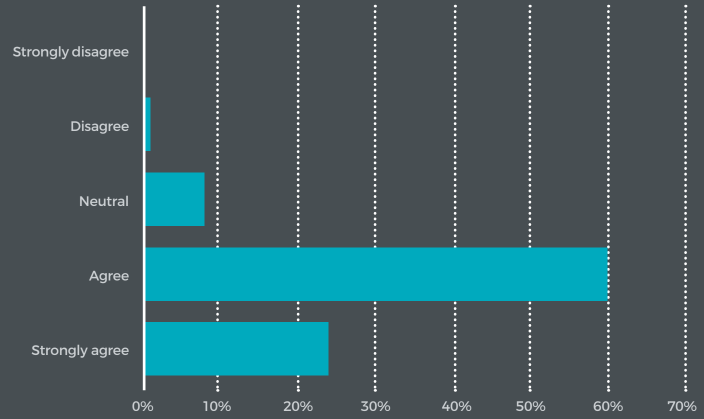
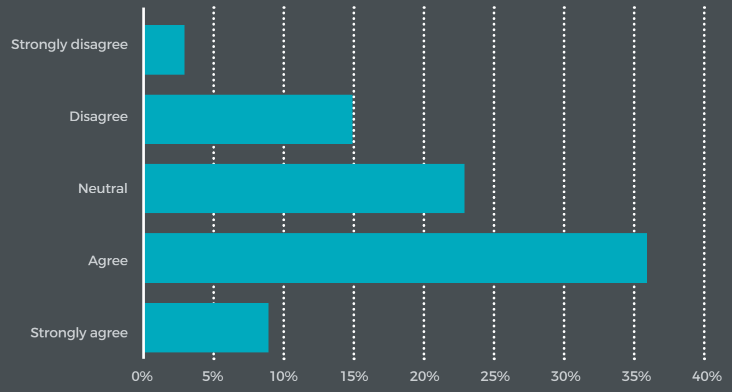


Figure 5: New technologies are enhancing understanding

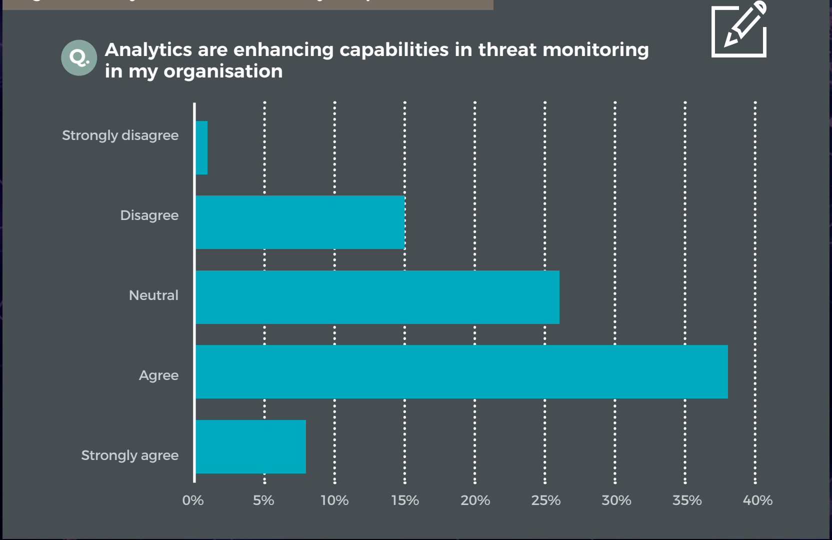
Q. My organisation is investing in technologies that enhance our understanding of the dynamics in our environment and deliver greater visibility



> In the case of cyber threats, it can reduce and prioritise the workload of analysts, manage incident response and workflow, and reduce detection and response time.

It is important to be mindful that purchasing a new technology is not in itself a solution to improve threat monitoring. In order to put in place the human processes to utilise and analyse the output, organisations will require a multi-disciplinary skill set within their security and risk teams. This includes how to use technology for threat monitoring and risk analysis as well as how to deal with the complex connectivity of topics such as geopolitics, terrorism, economic risks, cyber security and so on.

Figure 6: Analytics tools are valued by risk professionals



> **Purchasing a new technology is not in itself a solution**

Upskilling

While new technologies and analytics are increasingly accepted as beneficial and are being embraced by organisations for the purpose of threat monitoring, when it comes to training and upskilling the security and risk teams there remains work to be done.

Many organisations still rely on off-the-shelf training programmes for their intelligence and security specialists that are not tailored to the relevant risks and threats. Given the complex landscape that risk and security teams are facing today, organisations need to focus on the appropriateness and quality of training and technology applications that are pertinent to their specific needs rather than the quantity that is purchased.

It is only by putting in pace the relevant training, upskilling individuals and providing direction for the teams using the technology on a day-to-day basis that a return on investment (ROI) will start to be seen.

Figure 7: More training is needed to utilise new tools

Q. My organisation is investing in training so that analysts can make greater use of all the data and analytic tools available to them

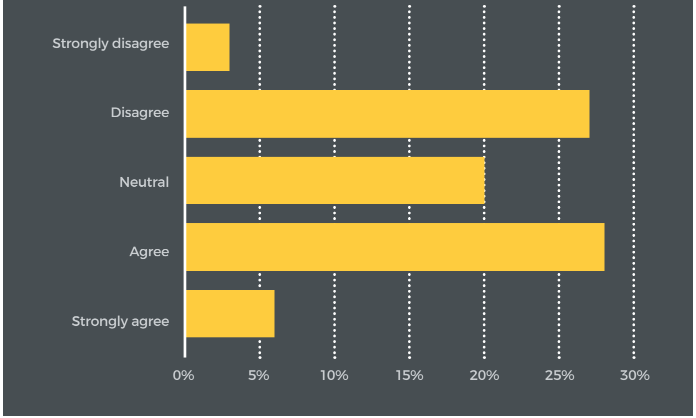
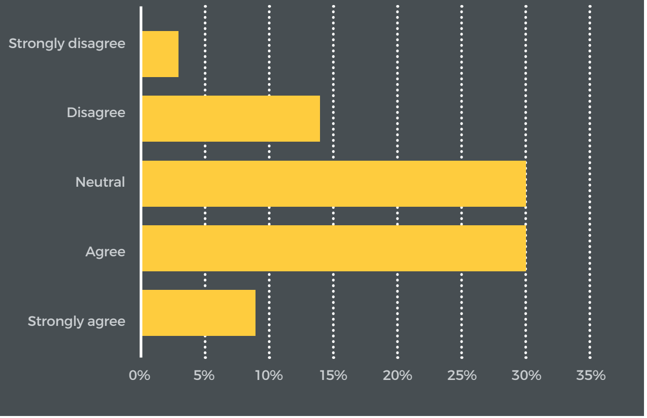


Figure 8: Organisational culture change is required

Q. My organisation appreciates the operational and cultural changes required to maximise the true value of threat monitoring



> **Organisations need to focus on the appropriateness and quality of training**

Turning risk into reward

The biggest challenge most risk, intelligence and security teams face today is that the quantification of ROI is extremely difficult when the job is to prevent something from happening. Risk management and security remain cost-centres for most organisations rather than being viewed as adding value.

When articulating the benefits internally, the focus should not start and end with the prevention and mitigation of events that come into contact with the organisation. To achieve buy-in, leadership and investment from the C-suite, it will want to see how the tools and strategy can be deployed to unlock more potential and new opportunities within the business. Getting them onside will be essential to put an effective and properly utilised system in place with collaboration across the organisation.

“We see the most effective results when the C-suite gets involved and the CRO, CSO/CISO, COO are working together. There is a trend towards this convergence, but it takes time to put in place because often security, IT and risk are not speaking the same language,” says Nicolas Reys, director of cyber security at Control Risks.

A good threat intelligence programme can generate new opportunities by identifying areas for development and innovation at a strategic level, allow more informed market entry decisions and provide real commercial advantages.

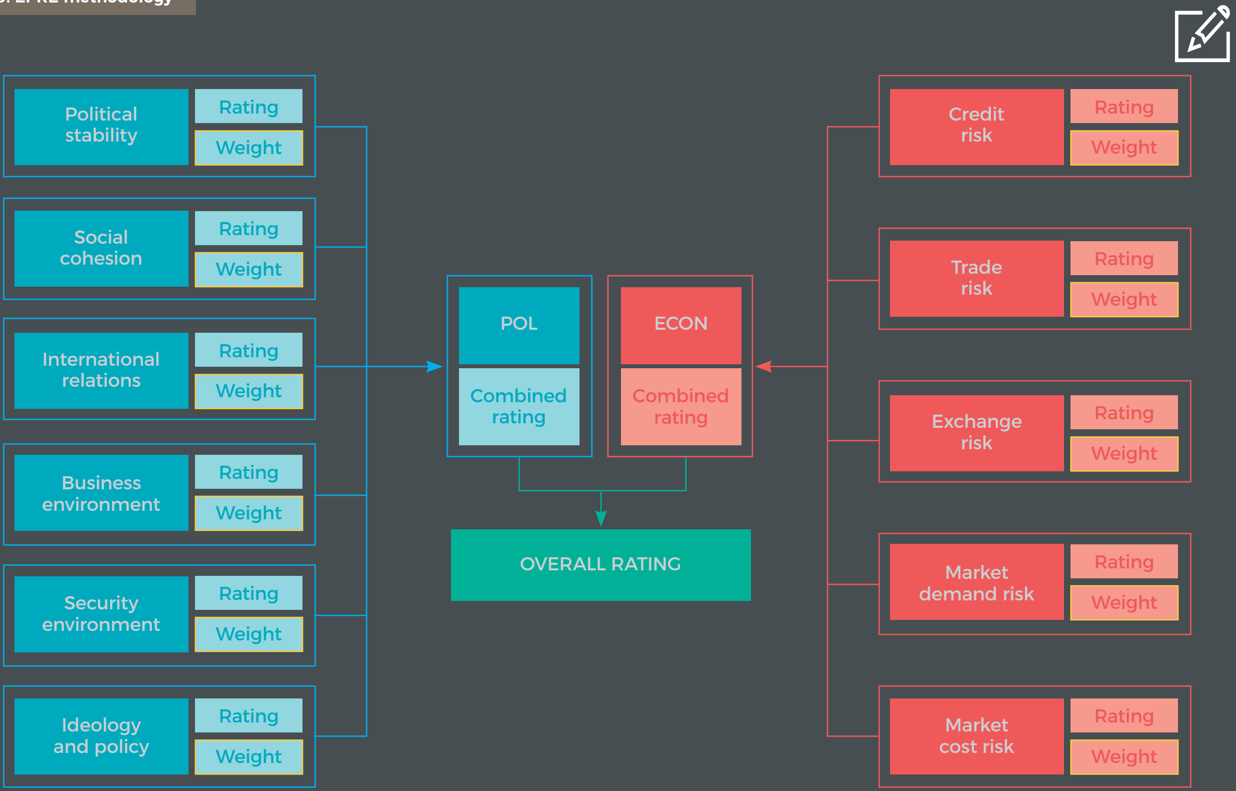
When finance and telecommunications businesses are confident in their cyber security systems, for example, to protect their customers’ valued data from cyber attacks, this can be promoted as a differentiator from competitors.

When organisations put in place a mature threat monitoring system concerning political risks in emerging markets, where they are already active or considering future investment, it may bring new opportunities to their attention when they arise. By monitoring the economic performance, political stability and security landscape of a >

> There is a trend towards this convergence, but it takes time to put in place

Nicolas Reys, Control Risks

Figure 9: EPRE methodology



Source: Control Risks and Oxford Analytics

>

country among other key factors, organisations can begin to assess the risk-reward balance and whether it warrants further exploration. Control Risks takes this perspective further in its Africa Risk-Reward Index which plot's each country's performance relative to its African peers. Its Economic and Politics Risks Evaluator (EPRE) methodology is shown on page 26.

Organisations should undertake an upfront assessment to determine the desired outcomes sought from the threat-monitoring function and weigh these up against the current gaps in their existing monitoring infrastructure to ensure a more effective investment all round. This should go beyond the concept that "better monitoring would be good for the business" to a more detailed assessment of what threat monitoring will actually deliver and how the results will be utilised across the organisation.

Connecting the objectives and goals of the organisation, while making it more secure should drive the use of technologies and any plans to install additional monitoring or use threat intelligence.

Business opportunities to realise from threat monitoring

Informed market entry

Present competitive advantages

Anticipation of market trends

Risk-reward analysis

Key takeaways

- Engage senior leaders on the benefits of threat monitoring
- Take a holistic approach by collaborating across functions
- Identify and prioritise the key threats to the organisation
- Implement a monitoring system that recognises indicators and triggers response
- Utilise appropriate technologies and provide training to internal analysts

Control Risks

About Control Risks

Control Risks is a specialist global risk consultancy that helps to create secure, compliant and resilient organisations in an age of ever-changing risk. Working across disciplines, technologies and geographies, everything we do is based on our belief that taking risks is essential to our clients' success. We provide our clients with the insight to focus resources and ensure they are prepared to resolve the issues and crises that occur in any ambitious global organisation. We go beyond problem-solving and provide the insight and intelligence needed to realise opportunities and grow.

www.controlrisks.com

airmic

Airmic
6 Lloyd's Avenue
London EC3N 3AX
Phone: 020 7680 3088
Web: www.airmic.com

@Airmic

www.linkedin.com/company-beta/2254002

Control Risks
Mark Whyte
Senior Partner
mark.whyte@controlrisks.com

Control Risks
Cottons Centre
Cottons Lane
London SE1 2QG