Building a corporate security sandbox with publicly available information

How can corporate security officers identify and gauge the magnitude of events that could put a company's employees and assets in jeopardy? **Dataminr** has some pointers to address this daunting task

As companies expand their operating footprints to compete in global markets, they inevitably find themselves facing unforeseen situations. Mitigating the risk of operating in foreign locales, while ensuring the safety and security of employees and the protection of company assets, rests squarely with the corporate security department.

Nevertheless, how does a corporate security officer (CSO) identify and gauge the magnitude of events with the potential to put employees and the organisation's assets in jeopardy across the company's entire operating footprint? Although this is a daunting task for any corporate security team, for employees and executives working overseas it is, nevertheless, a basic expectation.

According to Tim Willis, Director of Europe, the Middle East and Africa for Dataminr, the pressure to compete globally continues to push companies into operating in unfamiliar markets: "We're seeing businesses increasingly sending people to parts of the world where they might not historically have done business," he says. Willis cites an increase in travel to politically unstable countries that are experiencing post-election violence as examples of why companies must possess the tools to gauge the conditions on the ground, and the potential risks for employees and executives in overseas markets.

Is the information from a journalist, news agency, government emergency first responder, the dark web, or is it chatter from members of the public?

While many corporate security departments dedicate resources to educating business travellers on dangers abroad, education is just one piece of the puzzle. Once companies venture outside the confines of their established markets, corporate security departments must possess the ability to monitor events for their potential to put employees in harm's way or impact the company's ability to operate.

But there are ways of adding realism to training. Thanks to the existence of a vast treasure trove of publicly available data, including social media posts on Twitter, personal and corporate blogs, the dark web, and sensors such as earthquake monitors and flight arrival and departure data, breaking events can be detected within minutes – or even seconds – of an incident taking place. Consequently, to equip a CSO with the latest information on events occurring within the company's operating footprint, corporate security departments often turn to technology solutions that can analyse such disparate data quickly and efficiently, and derive relevant security alerts.

Regardless of technological innovation, however, making security-related decisions based on publicly available data requires corporate security employees to have the necessary training and expertise. Unfortunately, while some corporate security training programmes prepare employees for such demands, many fail to simulate the rigours of real-life situations, especially when it requires the use of a new technology, such as alerts derived from previously untapped sources like the dark web and information sensors. Undoubtedly, additional data sources will emerge with the potential to provide corporate security departments with a clearer picture of events as they unfold.

To help corporate security departments embrace the use of publicly available data to inform their efforts, Willis recommends the use of historical alerts as the basis for realistic, scenario-based training. For instance, by providing training participants with an initial alert relating to a previous incident, a map showing where the incident took place, as well as the pictures and videos capturing the event, corporate security departments add a higher degree of realism to their training programme. Using this approach, participants respond to the event as if it were taking place in real time. The fact that employees can see the source of the data allows them to weigh the importance of the alert accordingly. "Knowing the source may change the required course of action," says Willis. "Is the information coming from a journalist, a news agency, a government emergency first responder, the dark web, or is it just chatter from members of the public?"

Using historical alerts challenges the class participants to determine the magnitude of the event, its potential impact on the safety of employees and executives in the region, and whether to notify senior executives of the incident, just as they would in a real-world scenario.

Although the use of social media alerts by corporate security departments is a relatively new development, it is proving invaluable in helping CSOs monitor the threat landscape. When the corporate security department incorporates training on the use of content gathered from a range of publicly available sources, it accomplishes three goals:

- Since instructors know how the event unfolded, the selection and analysis of a previous alert allows the training team to pick a suitably challenging scenario to test the class;
- Conducting retrospective analysis allows the corporate security team to revisit how it handled an incident to derive lessons learned. For example, a company may view its decision not to close an office near an incident as a misstep. Alternatively, a decision to end an executive meeting early and require participants to shelter in place may now appear overly cautious; and
- By using content gathered from social sites, blogs, the dark web, and information sensors in a training environment, the CSO, members of the training cadre or training participants themselves may uncover more effective ways to manage, interpret, and disseminate the information derived from such alerts.

When corporate security departments embed historical alerts as a component of their training programme, they add a degree of realism that can often be missing from traditional approaches to security education.

And while there is no substitute for the challenges associated with an actual event, by using historical, real-time alerts, the corporate security department can improve the preparedness of its employees to make prudent decisions under pressure. C·RJ

Partner info

DATAMINR *is a technology platform that creates real-time, actionable alerts from publicly available information, and a Key Network Partner of the* Crisis Response Journal

■ *More details from: www.dataminr.com*

Daniil Peshkov |123rf