How Cyber Threat Intelligence Empowers the C-Suite

Cyber threat intelligence teams who understand the relevance of risk management practices can influence C-suite executives and board members more effectively. Here's how.

By Dr. Jamie Collier, Senior Threat Intelligence Advisor, Mandiant (part of Google Cloud) and Cameron Sabel, Senior Analyst, Intelligence, Mandiant (part of Google Cloud)

Cyber threat intelligence (CTI) typically is associated with operational use cases around the security operation center, yet its potential to reach executives is often left untapped. By harnessing strategic threat intelligence, security leaders can influence their C-suite and board more effectively.

Speaking the Language of Cyber-Risk

Dry and prosaic intelligence reports stuffed with dense technical details will never grab executives' attention. Security leaders need to instead make CTI insights more accessible and relatable. When executives engage with cybersecurity issues, this is typically part of broader risk management discussions. Therefore, it's essential for CTI teams to also speak this language if they are going to work with risk professionals.

CTI can dramatically raise the quality of cyber-risk assessments that too often are lopsided: Organizations will routinely detail mission-critical risks related to assets, vulnerabilities, and business priorities yet lack robust metrics on the threats an organization faces. This provides an opportunity for threat intelligence to hone the relevance of risk management practices by providing dynamic updates on the threats impacting an organization's sector and region.

Macro Decision-Making

CTI can inform more than just risk assessments and can even play a role for executives in their broader strategic decision-making. Strategic intelligence reports cover a broad scope of activity and distill key takeaways by identifying the most significant trends and implications facing organizations.

This could include country or industry profiles that outline the most likely threats and serious scenarios facing organizations. Strategic intelligence can also be used to assess threats related to specific business challenges. For example, the risks associated with entering a new market, proceeding with a cloud adoption project, or collaborating with third parties.

Policy Planning and Prioritization of Resources

When creating or reviewing risk management and security policies, strategic intelligence can be a valuable tool to ensure that the most relevant cyber-risks are being addressed in company policy and resourcing. This allows for more informed resource prioritization and allocation.

Here, long-term strategic intelligence reports can inform executive and board-level decision-making for budgeting, technology investments, and expansion of international operations. Furthermore, by identifying the most relevant threats facing an organization, intelligence can help to identify security controls as well as drive internal security policy changes — all while providing clear justification and support for any proposed changes.

Situational Awareness During a Crisis

CTI usually is most needed during crisis periods where situational awareness is highly valuable. Whether it be the COVID pandemic or Russia's invasion of Ukraine, these crisis situations often prompt executives to want to better understand how current developments are impacting the threat landscape. Here, an up-to-date view on threats facilitates the creation of policies for responding to major cybersecurity incidents and unforeseen global events. Risk reduction and intrusion remediation plans can be proactively created based on real-life data, potentially preventing or limiting damage caused by incidents, should they occur.

CTI is about identifying relevant threats, yet it has an equally important role in removing distractions during crises. Crisis situations invariably generate hype and sensationalist articles about hypothetical threats that can panic executives. For example, although there were countless articles warning about the elevated threats of COVID-related phishing in March 2020, Mandiant analysis revealed pandemic content only featured in around 2% of malicious emails at the time. Rather than lurch from headline to headline, threat intelligence provides metrics to help organizations make evidence-led decisions and avoid overcorrection.

Delivering Value as a Security Function

CTI can be leveraged across a security function, yet strategic intelligence use cases will deliver value far beyond the security department. Using CTI to deliver value to executives will not just elevate the role of intelligence but highlight the broader return on investment that cybersecurity teams can make to risk management, strategic decision-making, and crisis response.