BLACKBIRD.AI

The Executive Protection Checklist for Combating Narrative Threats on Social Media

Social media and narrative threats are a stark reality for today's executives. Boost protective narrative intelligence and executive protection programs with this checklist.

Executives are leveraging the opportunities social media has to offer, including networking and brand building. But with those opportunities come risks and a variety of social media threats, including dangerous, harmful narrative attacks – all of which can result in serious reputational, financial, psychological, and physical harm. However, there are steps that teams can take to mitigate the risk of these threats, thus boosting their protective intelligence and executive security programs. Here are some of the best questions to ask when evaluating an AI-based Narrative Intelligence Platform.

ACCESS CHECKLIST

Limiting access to executive and corporate accounts is the first step in social media-related executive protection. We recommend the following:

- ❑ Identify executive and corporate social media account users and ensure only authorized users have account access.
- ❑ Audit the authorized account access list with access regularly (we recommend at least quarterly).
- ❑ Implement a formal process of suspending social media account access from anyone who leaves the company (employees, consultants, vendors, etc.).
- ❑ Develop password policies and train on best practices, starting with the basics: 12-15 characters, a mix of upper- and lower-case letters, numbers, and symbols, and avoid personal information (birthdays, pet names, etc.).
- ❑ Ensure that passwords are updated regularly and whenever unauthorized access is suspected.
- ❑ Enable multi-factor authentication (MFA) for an extra layer of security. This requires two or more forms of verification (e.g., password + fingerprint, password + code) sent to a device.

TRAINING CHECKLIST

Training executives about social media attacks, including narrative attacks, is essential to executive protection. Security teams should include the following as part of a robust training program:

- ❑ Train users on social media platform security settings (such as limiting their general audience and who sees posts, blocking, disabling comments, and restricting access from third-party apps).
- ❑ Training should also include audience specifics on sorting "friends" into groups and adjusting access permissions appropriately, with "untrusted friends" receiving the lowest access. As part of this training, instructions on verifying "friend" requests should also be included.
- ❑ Include training on general online safety, such as how to spot malicious links and phishing attempts.
- ❑ Ensure that users understand the risks and threats they will face on social media, including deepfakes and narrative attacks, and how to identify and report them.

POLICIES AND PEOPLE CHECKLIST

Executive protection is more than limiting access and conducting security training. We recommend including a human-centric approach with guidance to executive protection:

- ❑ Create a culture of security by ensuring that executives and their inner circle understand how their activities and the online activities of those with whom they associate can make them vulnerable to social media attacks.
- ❑ Empower executives, friends, and their families to have online security conversations with their respective circles. This can include asking friends and colleagues not to tag them or share their locations, photos, or other personal information on social media.
- ❑ Establish clear and security-focused social media policies. In addition to general social media best practices, these should include:
  - ❑ Guidance for executives on posting about political and social issues, especially those considered controversial.
  - ❑ There are parameters regarding what can and cannot be shared via executive or corporate accounts, including personal, executive-focused details that can lead to phishing attacks or physical confrontations.
  - ❑ Also, include parameters around the type of content/sentiment that should or should not be reposted and profiles that shouldn't be tagged.
  - ❑ Requiring delayed posting and tagging (e.g., waiting until after an event to tag venue and executives/notable attendees or posting vacation photos after returning home).

- ❑ Evaluating the background of photographs and videos for security risks before posting. This can include sensitive information on a whiteboard, documents sitting on someone's desk, or notable people walking past.
- ❑ A process for approval and additional guidelines from a communications officer for select updates, including anything potentially controversial or that could otherwise compromise executive security (e.g., posting around events).
- ❑ Turning off geolocation to prevent real-time check-ins and geotagged photos.
- ❑ Exercise caution when posting information about and photos of friends and family.

- ❑ Include family and staff in safety training, with sessions and modules that contain meaningful and relevant information for their activities.
- ❑ Extend the corporate social media security culture to the entire company, requiring training on social media best practices and identifying narrative attacks as part of security training.

THREAT LANDSCAPE AWARENESS AND RESPONSE CHECKLIST

Develop a process for monitoring the narrative across the information landscape, focusing on detecting coordinated narrative attacks.

- ❑ Create escalation protocols if an executive, staff member, or family member spots false narratives or receives threats.
- ❑ Stay current on the latest social media scams and threats, as well as trends in manipulated media, and incorporate these into updated training and messaging.
- ❑ Escalation protocols should include a physical security element for people and property.
- ❑ Develop an executive-security-focused rapid response plan. In addition to security escalation and protocols, communications teams should have internal and external messaging ready.
- ❑ Partner with a narrative intelligence expert. These experts monitor the entire threat landscape and find the who, why, and how behind narrative attacks before they go viral, boosting protective intelligence and helping executive protection teams make better, more strategic decisions.

NARRATIVE INTELLIGENCE IS PROTECTIVE INTELLIGENCE

- ❑ What are the most harmful narratives that can impact our executives?
- ❑ Am I aware of the contagion effect of the narrative across networks?

- ❑ Who are the hyper-agenda-driven threat actors, cohorts, and communities behind the narratives?
- ❑ What is the bot-driven manipulation that scales them?

Narrative intelligence teams have advanced technical capabilities to map the networks harmful social media attacks and narratives touch, the anomalous behavior that scales them, and the cohorts and communities that connect them. This enables organizations to understand narrative threats as they scale before they gain traction and become harmful - a critical element to strategic decision-making and response. The most effective social media and narrative intelligence measures require examining the entire threat landscape, from social media platforms to community chat rooms to news sites and even the dark web - to give you a comprehensive view of your executive and company risk profile.

Take control of your executive protection strategy today—schedule an executive threat and risk assessment now.

ABOUT BLACKBIRD.AI

BLACKBIRD.AI protects organizations from narrative attacks that cause financial, reputational, and physical harm. Our AI-driven Narrative Intelligence Platform identifies key narratives that impact your executives/organization/industry, the influence behind them, the networks they touch, the anomalous behavior that scales them, and the cohorts and communities that connect them. This information enables organizations to proactively understand narrative threats as they scale and become harmful for better strategic decision-making. A diverse team of AI experts, threat intelligence analysts, and national security professionals founded Blackbird.AI to defend information integrity and fight a new class of narrative threats. Learn more at Blackbird.AI