HOW TO KEEP YOUR ORGANIZATION SAFE

ON SOCIAL MEDIA

The case for a social media security strategy

If your organization has been in existence for more than a few years, your brand likely retains a mature risk management structure. But does that extend to social media? Lax oversight of brand-owned social media accounts can harm your brand.

The power and importance of social media is irrefutable. Incorporating social media into an overarching business marketing plan can increase market reach, build brand loyalty, and keep your brand top-of-mind. Social media also facilitates fast communications, low-effort content promotion opportunities, and CapEx savings. Targeted, paid social media ads can inspire further brand awareness.

"Organizations that do not include social media in their business strategy run the risk of losing relevance in the market," states the professional human resources membership organization, SHRM.[1]

Yet, despite the opportunities inherent within social media, the absence of a social media security strategy can expose your brand to risk. Be risk-resilient. Develop a social media security strategy that prioritizes policies, administrative oversight, and security technologies that can protect your assets.

[1] Managing and Leveraging Workplace Use of Social Media, SHRM

Develop a social media security strategy that prioritizes policies, administrative oversight, and security technologies that can protect your assets.

What is the risk?

On the surface, social media channels come across as innocuous and almost playful environments. But, attackers have become facile with social media-based deceptions. From spam, to the manipulation of your content, to the impersonation of your accounts, cyber criminals lurk, backstab and hack via social media platforms.

A few short years ago, a Twitter attack conducted by nation-state backed operatives resulted in the distribution of malware within the US Department of Defense.[2] The attack was contained, but should it have spread, it could have led to extensive disruption.

Despite social media's obvious advantages, it can also expose enterprises to risk. Risks include phishing, spear phishing, malware, account takeover, doppelganger accounts, and more. Mitigating such risks requires the prioritization of a social media security strategy.

Social media risk governance: Policies

In developing policies and guidelines around brand social media channels and their management, include input from your employees. Keep any internally published material light and positive in tone. You may want to leverage infographics to communicate information – a move that underscores your understanding of what social media is about; having fun, being social, and "info-taining."

20%

20% of small-to-medium sized businesses have experienced social media compromise.[3]

[2] The Top 10 Worst Social Media Cyber Attacks, Spencer Wolfe, Infosecurity Magazine, Oct 2017

[3] *20% of small-to-medium sized businesses have experienced social media compromise*, Pia Bogush, BusinessTech Weekly, June 21, 2020

Ensure that your social media policies include information about what types of proprietary information can and cannot be shared on social media, who manages the accounts, who ultimately owns the accounts, use of common sense, an outline of specific security protocols, and include a plan-of-action in the event of a security or public relations catastrophe.

Within your social media policies, consider developing a sub-policy pertaining to social media data collection. If posting content on social media, your brand inherently collects user information pertaining to likes, followers, and shares. Depending on the nature of your business, your brand may also take in and reuse User Generated Content (UGC). Strong data and privacy protection policies can be a brand differentiator.

At the end of the day, a brand's social media governance policies need to clarify information pertaining to security. Think of your overarching policy document a "living" document, and encourage appropriate updates as social media use, platforms, and capabilities continue to evolve.

Social media risk governance: Administrative management

When it comes to managing internal usage of your social media channels, select an employee or a group of employees to serve as social media administrators. Appointing social media administrators or managers can cut down on errors and can ensure that suspicious requests, behaviors...etc., are handled efficiently and appropriately.

Advise social media administrators to obtain permission from employees, clients or business partners ahead of publicly publishing their images or names. In addition, social media administrators should adopt a strong password policy and two-factor authentication in relation to all business-owned social media accounts. Also, be sure to provide social media admins with cyber security training, especially as it pertains to phishing.

> Your account managers are vulnerable to social media attacks. According to Check Point Software, 52% of all phishing threats, globally, during Q1 of 2022 targeted LinkedIn account owners. Account managers should understand what phishing, spear phishing and other threats can look like.[4]

[4] *How 52% of phishing attacks reel in sharp and savvy LinkedIn Users*, CyberTalk.org, April 21, 2022

On a bi-annual or annual basis, request for admins to conduct a social media audit. Ensure that other entities, including cyber criminals, are not using your brand's name or image for unintended purposes. For example, hackers have been known to set up 'support' accounts in a brand's name. In conducting an audit, also scan your competitors' social media channels to identify any security snafus or stumbles that your brand would not want to encounter.

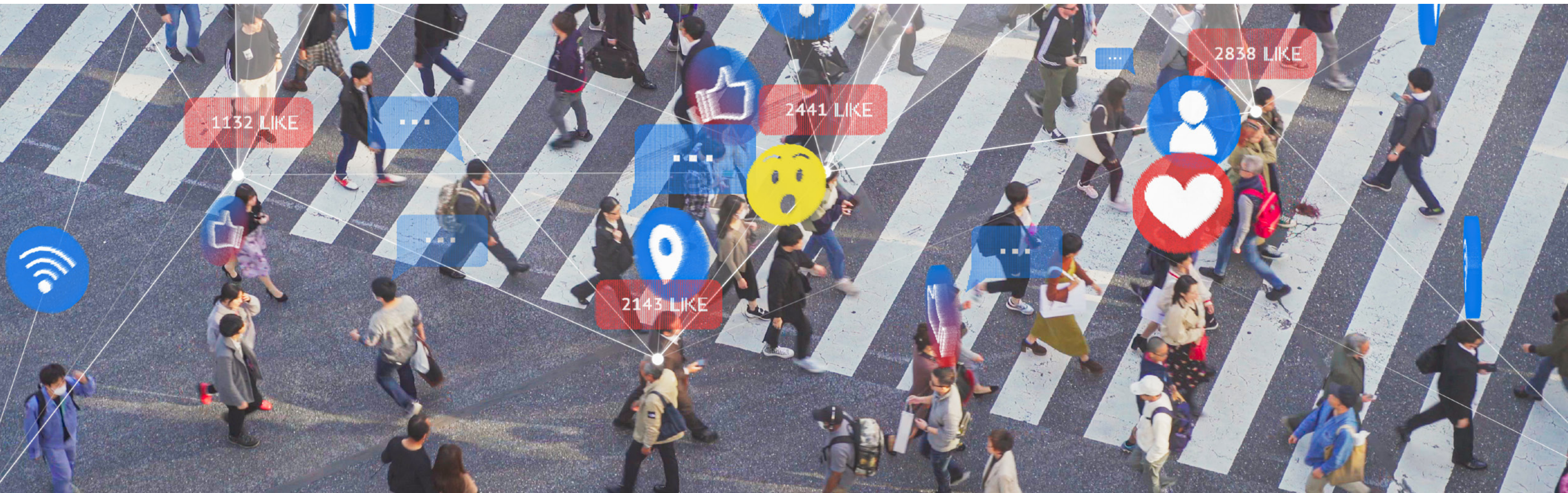
Further, consider adopting social media management tools. These can help your brand create a content approval pipeline and compliance checks, which will enable social media account managers to easily spot any unexpected posts indicating a hack or an error. Social media management tools can also help reinforce the least-privileged access administrative model.[5]

Social media risk governance: Technology

Once your brand has the foundational elements of social media risk governance in place, ensure that your technology also supports your strategy. Set expectations around keeping corporate devices and business-owned software updated and patched. Deploy anti-malware and/or endpoint protections on devices. Network perimeter security also needs to be in place in order to protect any information collected via social media and that receives offline analysis. Invest in a comprehensive security product that can help you block a broad array of threats.

> Invest in a comprehensive security product that can help you block a broad array of threats.

[5] Least Privilege Access, Cyber Hub, Check Point, 2022



Don’t risk it

Not sold on the need for social media risk governance? Imagine that hackers found a means of posting fake news under a major media outlet’s social media account or handle. Theoretically, hackers could post a story about a fake geopolitical event, such as a maritime battle or a bombing. Left unchecked and undiscovered, such news could precipitate real-world physical violence, with devastating consequences. Don’t let your brand become a catalyst for a crisis. Keep your social media accounts secure.

Conclusion

The biggest risk to your brand’s social media image may be complacency. Not taking any action around social media risk governance could lead to damaging consequences. Ensure that your organization retains a strong social media policy, administrative management protocols, and security technologies that can support the safe and continuous use of social media channels.

If social media is an essential component of your marketing strategy, social media governance shouldn’t be an afterthought.

For more business and cyber security insights, visit CyberTalk.org.

Worldwide Headquarters
5 Ha’Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com