From the desk of
Thomas F. Duffy
MS-ISAC Chair

Social Media: The Pros, Cons and the Security Policy

Risks & rewards of social media

Social media is a great tool in your organization's communications toolbox. Many Americans have accounts on at least one platform and expect to find pages for their favorite brands and communities. If used correctly, it can have many benefits:

- **Providing real-time information.** Social media enables organizations to provide information in real-time. This is especially useful if your organization needs to communicate important information quickly. For example, if your organization experiences a time sensitive incident, such as a data breach, you can use social media to share pertinent information and provide steps your followers can take to remediate the damage. Government entities can use social media to disseminate information about programs and public meetings, changes in schedules, road work, and other information that constituents need to know about.
- **Answering questions**. Social media allows consumers to ask organizations questions and provide feedback. This means you know what information and product features they want, what you are doing well, and where you can improve. You can change your customer service processes, add new products or change existing ones, or keep doing what you do well. Most importantly, you can be responsive to your customers, which will help grow your image and your business.
- **Humanizing your organization.** Consumers can get to know your brand and the people behind it, and vice versa. Because the conversation is person-to-person and not bot-to-person, a company can reach customers using social media in ways that other marketing and advertising can't. For example, you can adopt a more human voice through social media than you would through traditional advertising. Even a simple "Please PM your information so we can look into your concern" can go a long way toward keeping a current customer happy and maybe getting some new ones.

Of course, the unicorn is the post that goes viral for the right reasons. However, not everything looks rosy when it comes to organizations using social media.

Building a security-focused social media plan

Privacy and security risks associated with social media platforms only increase as the number of users and platforms grow. Cybercriminals mine social media accounts to get valuable intelligence that they can use in malicious campaigns. All organizations should develop a social media policy that takes cybersecurity and privacy into account. The first step is to develop a social media policy that includes what can be posted, who can post, and on what devices (e.g., can they use their personal device, or does it have to be a company-owned device?), and who is responsible for keeping and changing passwords. These are just some of the things that should be addressed; there are guides that will help you write a detailed plan.

Below are a few tips for developing a secure social media plan in your organization:

- Establish a social media team headed by a senior person. This person will be responsible for implementing and enforcing your company's social media policy, as well as issuing access to those who need it. The team should include someone from the IT department who can consult on risk mitigation and who can assist if security issues arise.
- Use role-based email addresses instead of employee addresses. Using email addresses like social@company.com and communications@company.com makes it harder to break into a network. A cybercriminal needs two email addresses to

figure out your company's email assignment scheme, which is a valuable piece of information needed to break into your network or your building.

- Your plan should include a way to insulate employees who choose to participate in your social media campaign. They should consider setting up separate social media accounts for work that are not linked to their personal accounts.
- Unless the employee has agreed to participate in a social media campaign and has taken steps to insulate themselves, try not to identify employees by more than one identifier, such as name and department, or name and email address. For example, if you post a photo of an employee who has earned an award, avoid identifying them as Jane Smith from Accounting. A criminal can use this information to get into the building ("I'm here to see Jane Smith from Accounting") or find her and her email address in the company directory.
- Any employee photos on social media (or any public-facing website) should be taken in a closed conference room or some other area away from active workspaces. This will prevent confidential information, employee names, or information on screens or desks from inadvertently being photographed.
- Consider a policy of zero trust and require that all posts be vetted by the social media team for content prior to publishing.
- Review your social media policy at least quarterly. Go over the privacy settings for each platform and make any necessary changes. Make sure only the people who need access and publishing privileges have them, remove anyone who does not, and change privileges as needed. Sit down with your IT experts and discuss the latest threats to make sure you're covered. Finally, take a look at your overall social media policy to ensure that it's the best for your organization and make any necessary changes.

Securing our connected future

Social media has proven to be a powerful communications tool for both business and government organizations, but its powers can be used to harm as well as help. A solid social media policy and security plan that is implemented with care, will vastly improve your social media strategy and protect employees' privacy.