Road Hazards: Recognizing the Risks of Social Media

By Gadi Ben-Yehuda

The advent of social media has opened up new roads on which digital brigands operate, but the methods that they use are decades (if not centuries) old. One of the most effective means to diminish the risk is to develop, enforce, and routinely update a social media use policy. By doing so, agencies can greatly decrease the likelihood of highway mishaps.

Responding to the Risks

There are four main risks that agencies face when their employees are active in social media: stolen data, damage to devices or networks, diminishment of reputation, and loss of employee productivity. In response, agencies need to take steps to safeguard their data, secure their networks and devices, protect their online reputation, and maintain high productivity.

It is always tempting to focus on addressing particular vulnerabilities, such as infected e-mail attachments. A successful policy, however, should start with a clear understanding of what it intends to prevent—that is, it should focus on outcomes rather than methods. After all, the methods used to attack or disrupt agency systems and networks are fluid—the only constant is change. Threats are likely to change as quickly as new social media are introduced and new security loopholes are discovered (or created).

Arriving at desirable outcomes on a daily basis requires the coordination of agency leadership, IT staff, and all employees who use social media. A carefully crafted policy that all understand and follow will minimize the risks associated with using social media—providing necessary guidelines to reap its benefits while avoiding its perils.

Safeguarding Data

Robin Hood was perhaps the most famous highwayman. Though he would relieve rich travelers of their valuables, he allowed them to pass otherwise unharmed. Today's corollary is the hacker who breaks into networks and devices and steals the data they contain.

Data thieves have three main tools at their disposal. The first is malware, a portmanteau of malicious software, examples of which include viruses, worms, and trojans. Through malware, hackers can disable or bypass security protocols, record and transmit keystrokes, access sensors (such as cameras) on network-connected devices, or simply have data transmitted directly to them. The second tool available to hackers is accessing a network directly, either through guessing passwords, applications that run so-called alphabet attacks, or exploiting networks' vulnerabilities. Finally, hackers use social engineering to gain access to secured networks and devices.

Social engineering is a relatively new term for a centuries-old art. It involves winning someone's trust to trick or coerce them into divulging information or performing an action. Examples of social engineering might be sending someone a link through Twitter that then takes them to a malicious website. Another non-digital example might be calling

Gadi Ben-Yehuda is the Innovation and Social Media Director for the IBM Center for The Business of Government.

someone in their office and impersonating a member of the IT staff and acquiring the person's logon information.

Social media have added new methods for all three types of attack. Professor Alan Oxley's recent report, *A Best Practices Guide for Mitigating Risk in the Use of Social Media,* published by the IBM Center for The Business of Government, details the many steps organizations can take to avoid a data breach, whether from malware or social engineering.

The most important step to safeguarding data is to develop a comprehensive social media use policy, which raises employees' awareness of the risks posed by social media and provides them with strategies to mitigate those risks.

Securing Networks and Devices

Sometimes, highwaymen target the vehicles—regardless of their contents—while others care less for the vehicles and command the actual road itself. The parallel in the digital world involves hackers who seek to control whole terminals by hijacking their systems and turning them into "bots" on a "botnet" that may then attack a third network, or by seeking to bring down entire networks out of malice or for some personal gain.

Network security companies such as McAfee and Kaspersky are constantly updating their virus protection databases with new viruses, but no software can protect systems from attacks that target not a computer, but the computer's user. For example, in the early 2000s one such attack came in the form of an e-mail sent to people by their friends: *"[T]his virus has probably forwarded itself on to you. It is easily removed if you don't open the file (jdbgmgr.exe). It has a teddy bear icon and is not detectable by Norton or McAfee. First go to Start then the find or search option. In the files or folders option type jdbgmgr.exe. … [T]he virus has a grey teddy icon. DO NOT OPEN IT. Go … to file (on the menu bar) and DELETE…"*

Though deleting that particular file did not pose a security risk, it would be every bit as easy to write a hoax e-mail that unaware users could follow to the detriment of their systems and networks. As with securing data, employees must take seriously the potential threats to their devices and the networks that support them; it is critical to understand the importance of securing their devices and working with their IT staff to implement and follow the use policies set by their leadership.

Protecting Online Reputations

When engaging with the public online, an agency is risking not only its digital assets, but its most important social asset: its reputation. In February 2011, the Red Cross became an example of how a single 140-character communication could undo much of the good will the organization had built up. That day, a tweet was sent out on the Red Cross's official feed that read: "Ryan found two more 4 bottle packs of Dogfish Head's Midas Touch beer … when we drink we do it right #gettngslizzerd." Thankfully, the Red Cross

communications team turned what could have been a public relations nightmare into a marketing dream, when they tweeted "We've deleted the rogue tweet but rest assured the Red Cross is sober and we've confiscated the keys."

In the summer of 2012, The Altimeter Group released a research report, "Guarding the Social Gates: The Imperative for Social Media Risk Management," which found that organizations rank damage to their reputation as the primary risk posed by social media. The best way to manage this risk is the same one used to avoid traffic collisions: teach safe conduct on social media and have regular training sessions. For example, the U.S. Environmental Protection Agency (EPA) has developed a flow chart that helps its employees decide whether to ignore or respond to a social media message. Finally, it is vital to instill in all employees the understanding that their online behavior, especially at work, reflects on the organization.

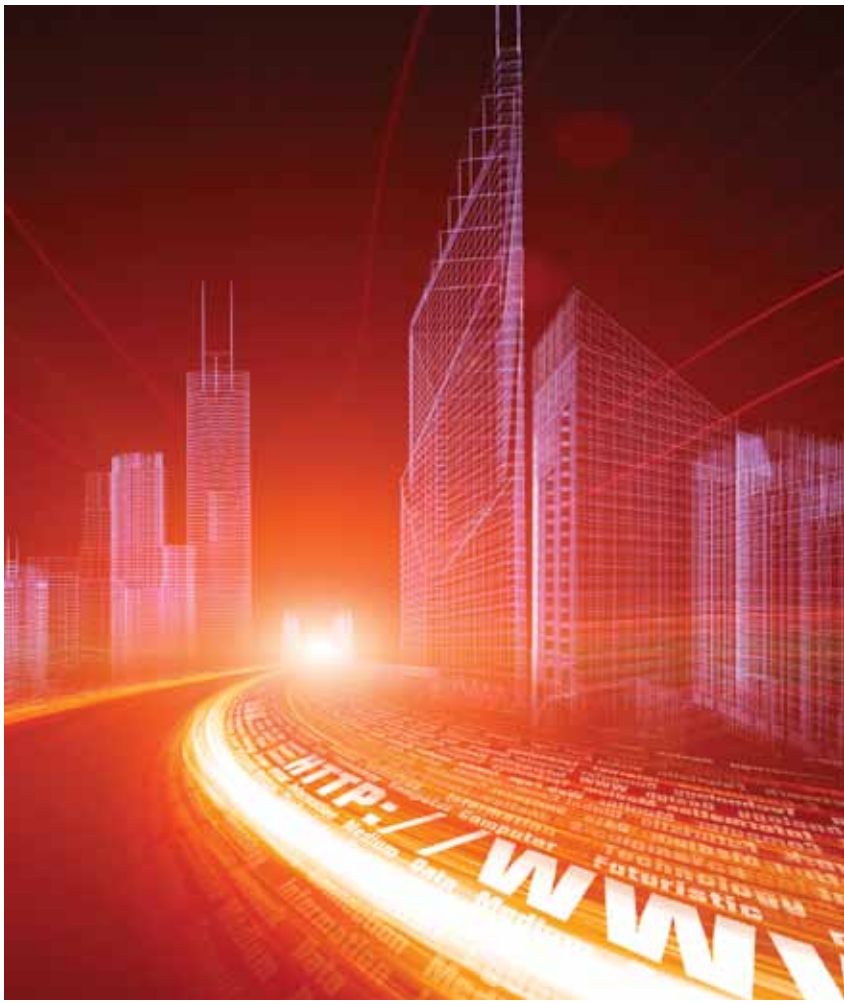
Maintaining High Productivity

Sometimes what impedes productivity is not a bad actor at all, but the many distractions of the road itself. Scenic overlooks, or the rapturous tableaux of foliage in early autumn, can cause even the most conscientious drivers to pull over for extended periods of leisure.

On the digital highways, personal e-mail, social games, and even distractions in the guise of news and information are always only a click away. Further, even as mobile devices have allowed work to seep into the home, they have also allowed personal activities—from shopping to trading stocks to commenting on a friend's wedding photos—to enter the workplace.

The solution cannot be to ban personal connectivity devices, but rather to set productivity milestones and hold employees accountable for reaching them. In 2010, Washington, D.C.'s Office of the Chief Technology Officer began implementing a program called ROWE (Results Only Work Environment), which allowed employees literally to set their hours, but made them entirely responsible for accomplishing specified tasks in a set timeframe. That experiment was prematurely cancelled, so no evaluations were possible.

However, a University of Minnesota study of Best Buy's ROWE programs demonstrated a 45 percent drop in employee turnover, and the company itself noted a 35 percent increase in productivity among participants. Social media tools made this program possible by enabling employees to collaborate easily.



New Rules for New Roads

Social media have become indispensable channels both for government agencies seeking greater citizen participation and for citizens and organizations looking for ways to participate in their own governance. Though sites like Facebook, Twitter, and YouTube present new perils, those risks can be managed; and properly mitigated, they can never outweigh the benefits of these powerful new tools.

To operate safely, agencies need only learn the rules for this new road.