In Websense's annual *Threat Report*[12] they look at organizational threats coming from the Web, social media, mobile devices, e-mail, malware, and data theft. The following are six key points from their report:

1. **Web Threats**—The Web became significantly more malicious in 2012, both as an attack vector and as the primary support element of other attack trajectories (e.g., social media, mobile, e-mail). Websense recorded a nearly sixfold increase in malicious sites overall. Moreover, 85 percent of these sites were found on legitimate web hosts that had been compromised.
2. **Social Media Threats**—Shortened web links used across all social media platforms hid malicious content 32 percent of the time. Social media attacks also took advantage of the confusion of new features and changing services.
3. **Mobile Threats**—A study of last year's malicious apps revealed how they abuse permissions. Especially popular was the use of SMS communications, something very few legitimate apps do. Risks also increased as users continued to change the way they used mobile devices.
4. **E-mail Threats**—Only 1 in 5 e-mails sent was legitimate, as spam increased to 76 percent of e-mail traffic. Phishing threats delivered via e-mail also increased.
5. **Malware Behavior**—Cybercriminals adapted their methods to confuse and circumvent specific countermeasures. Fifty percent of web-connected malware became significantly bolder, downloading additional malicious executables within the first 60 seconds of infection. The remainder of web-connected malware proceeded more cautiously, postponing further Internet activity by minutes, hours, or weeks, often as a deliberate ruse to bypass defenses that rely on short-term sandboxing analytics.
6. **Data Theft/Data Loss**—Key changes in data theft targets and methods took place last year. Reports of intellectual property (IP) theft increased, and theft of credit card numbers and other personally identifiable information (PII) continued to grow. Hacking, malware, and other cyber threats continued to be a common method of attack.

Case Discussion Questions

1. After seeing the impact of the hacked Twitter account, would news organizations become even more attractive targets? Why or why not?
2. Could an insider use the fact that news feeds are scanned for trading decisions to manipulate the stock market? How?
3. How could highly integrated information systems be a threat to corporations?
4. Could a subcontractor with weak security practices make a corporation more vulnerable? How?
5. Why would web threats see such a drastic sixfold (600 percent) increase?
6. According to the Websense report, how were attackers using social media?
7. How can malware writers adapt to software detection techniques?
8. How can organizations limit their exposure to malware?

rspective Questions

What was the most surprising thing for you in this hapter?

2. What was the most difficult material in this chapter for you?

ense Inc., *Websense Threat Report*, February 13, 2013. https://www.websense.com/content/websense-2013-threat-spx.