Statements about cybersecurity: A duty of accuracy or a license for puffery?

By John Bandler, Esq., Bandler Law Firm PLLC

APRIL 14, 2025

Organizations need to make statements about their cybersecurity and information systems, articulated by different people to different audiences.

There are tensions because some parts of an organization sell and reassure, others work to keep information systems secure. Sometimes a single individual is called upon to do both, such as a chief information security officer (CISO).

To sell, the organization lets clients, customers, and investors know things are running great, their products and services are excellent, security is airtight. These rosy statements help make the deal happen.

Principles from legal compliance, efficiency, and ethics favor accuracy in communication. Accurate communications can be trusted and acted upon. Deception is generally improper and also creates inefficiencies.

To secure and operate, the organization needs facts not puffery, and few organizations are perfect.

In sum, there is a legal duty of accuracy with diligence required, plus an ethical and practical imperative.

Why we tell others about cybersecurity

Organizations make statements about their information systems for a variety of reasons:

Internal communication to assess and convey facts about current practices and risks, and desired changes and goals.

External communication for three main reasons:

- for *marketing*, to get others to buy the company's product or service (or continue doing so).
- for *investors*, to get them to buy or hold ownership in the company.
- for *contracts*, to provide information to a client or to obtain or maintain cyber insurance.

What we tell others — a practical and legal refresher

Principles from legal compliance, efficiency, and ethics favor accuracy in communication. Accurate communications can be trusted and acted upon. Deception is generally improper and also creates inefficiencies. Organizations need to be able to learn and assess facts, and this includes identifying deficiencies honestly to eventually correct them.

Some are motivated away from accuracy because it is easier for some to say what is convenient in the moment and avoid painful truths. Admitting deficiencies or mistakes can hamper an immediate sale or investment and provide ammunition to opponents.

The law has evolved to favor accuracy with three methods.

First, the hearsay exception for a statement by an opposing party means that a litigant gets to pick and use any statement made by the other side which might help their own case. These statements are evidence and can be worthy of mention in the complaint or opening statement. The other side is reduced to claiming the statements were "cherry picked" and "taken out of context."

Second, law and the process of litigation disfavors deception (in theory). Much of our legal process is about fact finding, and many of our laws and processes prohibit deceit.

Third, prior inconsistent statements are admissible for certain purposes, including to prove deception. When a person says opposite things at different times, that can be used to prove one of those statements was false.

Cyber insurance and other contracts

Contracts today may require questionnaires and statements about cybersecurity, information security, and privacy. These representations are relevant at contract formation and

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Thomson Reuters™

throughout the contract duration. Cyber insurance is one type of contract.

Some of the questions can be challenging, perhaps poorly worded, ambiguous, technical, or designed for a different sized organization.

The response always matters, and it should be accurate and clear. If a dispute ever arises it will be read in the *least* favorable light, under the harsh fault-finding gaze of an opposing attorney.

A simple question might be:

> "Does the organization use two-factor authentication on email systems?"

An accurate response is required (of course).

Other questions may present more challenges. While it might be convenient to check the "Yes" box, reality might be different, and a careful, accurate sentence might be helpful.

Statements, investor protection, and the SolarWinds case

The Securities and Exchange Commission (SEC) lawsuit against SolarWinds is a cautionary tale suggesting diligence for all statements about cybersecurity, no matter the audience.

The SEC alleges that false statements about cybersecurity protections are actionable under securities laws as deceptive to investors. The complaint was filed in October 2023, and I wrote about it soon after. ("SolarWinds and the SEC lawsuit" Reuters Legal News, Nov. 21, 2023, https://reut.rs/4j1ADub).

Since filing, the SEC filed an amended complaint in February 2024, SolarWinds made a motion to dismiss, and the Court ruled on this in July 2024.

The complaint is just an allegation, and the Court's decision rules only on the sufficiency of the complaint, not the merits of the case.

The decision allows claims to proceed based upon certain allegedly false statements made by SolarWinds in a cybersecurity statement they posted on their website before the data breach. This public statement of excellent cybersecurity included detailed specifics which were contradicted by internal statements. Some of the cybersecurity deficiencies arguably allowed the massive data breach which included access to SolarWinds systems and then to thousands of their customers.

The Court dismissed certain SEC claims that were based on SolarWinds statements of good cybersecurity made in press releases, blogs, and podcasts, deciding they were "non-actionable corporate puffery" and too general for a reasonable investor to rely on them.

The Court also dismissed claims based on alleged false statements made by SolarWinds after discovering suspicious activity, including how they characterized the event within their incident response activities, and external communications in the immediate period after the discovery.

Reading legal tea leaves based upon a single case is rarely wise, especially with pending litigation, and doubly so with a new administration with different regulatory priorities. Nevertheless, some practical and legal takeaways remain clear. It is problematic to be deceptive and to make inconsistent statements.

Here is how the Court summarized one sequence of events from Nov. 5, 2020 (in its decision of July 18, 2024, with citations to the SEC's amended complaint omitted).

Every organization needs to improve its cybersecurity, none can afford to rest on their laurels, and claim everything is perfect. Improvement happens only with honest discussion about the current state, to include deficiencies.

"In [a] group instant message, a [SolarWinds] employee raised whether to alert PAN [Palo Alto Networks] that there had been a prior attack... [SolarWinds] Infosec Employee F responded: 'I[' d] prefer nobody says on the call that we have seen something like this in the past.' Infosec Employee F then separately messaged [SolarWinds] Manager E, who agreed that SolarWinds should not disclose to PAN the previous ... attack. Later that day, on a phone call between SolarWinds and PAN, employees at PAN asked if SolarWinds had ever seen Orion [security software] act in this manner before. [SolarWinds] Infosec Employee F responded that they had not previously seen similar activity from the Orion platform. In contemporaneous instant messages sent during the call, Infosec Employee F messaged his colleague: 'Well I just lied.'"

Some may focus on the act of confessing to this dishonesty in a group chat. A deceitful person may take the wrong lesson — "*Do not admit deception in writing*." Some may question the organization's culture if employees felt free to discuss this duplicity with each other.

The main lesson for compliance and ethics should be clear: Be truthful in the first place, eliminating any need to discuss deception.

Given the dismissal of certain counts, it remains to be seen whether this sequence of post-breach statements will be admissible, but the lesson holds fast.

Benefits of clear and accurate writing and speaking

For good organizations working to do the right thing, there are benefits when employees, managers, and executives communicate clearly and accurately.

©2025 Thomson Reuters

Accurate facts are essential for good decision making, which helps to accomplish the mission, serve clients and customers, and stay in compliance with legal obligations. Accuracy and honesty about cybersecurity allows the organization to assess where it really is, so it can plan and navigate the course to where it wants to be. This adapted saying holds true today:

"*When we first start to deceive, what a tangled web we weave.*"

A deception may be convenient at the moment but creates complications soon enough. If organizations start to create a gap between;

- Rosy statements for clients, investors, and regulators, and
- Practical realities and facts needed to discuss and do the work of the organization,

then troubles brew. The greater the gap, the greater the risks of noncompliance, inefficiency, and future accusations of deception.

The lesson to learn is that facts and accuracy are good for the organization and for compliance.

Some will choose to learn the wrong lessons, such as "don't write anything down and limit what you say because it could be used against you." This approach cannot lead to efficiency and good management and starts down a slippery slope that is difficult to recover from.

Every organization needs to improve its cybersecurity, none can afford to rest on their laurels, and claim everything is perfect. Improvement happens only with honest discussion about the current state, to include deficiencies. That discussion will need to include the written word, because of the complexities of cybersecurity.

Sometimes we speak and write, sometimes we listen and read.

When we listen and read, we should temper our expectations to account for honesty. If we hear that everything is perfect, it might be too good to be true. If we hear about some deficiencies, we may want to have some forgiveness for certain defects if it means we are obtaining accurate and honest information.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the authors

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better protect and manage information systems. His latest book is "Cyberlaw: Law for Digital Spaces and Information Systems" (2025). His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on April 14, 2025.

© 2025 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.