CYBERCECURITY
DEFENDING YOUR ASSETS

Report: Why Technologists Fail to Communicate Effectively With Leadership

By Mitch Tanenbaum and Raymond Hutchins

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

In the midst of an obvious global cyber war waged by authoritarian regimes against the rest of us, why is it that so much of our IT infrastructure remains so vulnerable to attack?

Reasons for this include the complexity of the problem and lack of resources, but a primary reason is a breakdown in communication. Leadership is not effectively communicating with technologists and visa versa. This communication break-down unnecessarily exacerbates our security problems.

Some reasons for this communication breakdown include:

1. Leadership (aka boards and top management) still see cybersecurity as purely a technical issue as opposed to a business management issue. This out-dated attitude may apply to risk management and privacy as well. As a result, technologists (aka CIOs, CISOs, CTOs, IT Directors) may be segregated from leadership and may only rarely be required or expected to communicate with them.
2. Individuals in leadership are typically non-technologists who are not fluent in the technical languages spoken by their technologist subordinates.
3. There are natural barriers between non-technologist business leaders who are trained to communicate with humans and technologists that are trained to communicate with machines.
4. Technologists may not have the personalities and/or capabilities required to effectively communicate with leadership. They prefer interaction with technology tools and avoid management responsibilities and relationships. When their technology skills move them up the ranks, they are not prepared to communicate with management and leaders as equals. Leadership is sometimes forced upon technologists--sometimes this works...sometimes it does not.
5. Some technologists do not understand the importance of translating their technical languages into languages the leadership folks understand.

6. At times, some technologists may not want leadership to fully understand what is going on on the technology side of things.
7. Sometimes technology leaders, in order to protect their turf and power, may not communicate technology issues as candidly as they should.
8. Some technologists, knowing full well how smart and capable they are, may become resentful of higher ranking/paid folks who the technologist believes does not value or respect them enough.

About the Authors

 Raymond Hutchins Managing Partner rh@cybercecurity.com 303-887-5864	 Mitch Tanenbaum CISO/Partner mitch@cybercecurity.com 720-891-1663

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/

Did you find this position paper of value? Here are some of our other papers and reports:

1. The Global Cyberwar and Societal Response
2. Privacy Laws: An Executive Overview
3. Hiring, Managing and Firing MSPs
4. Caremark and More Propel New Board Risks