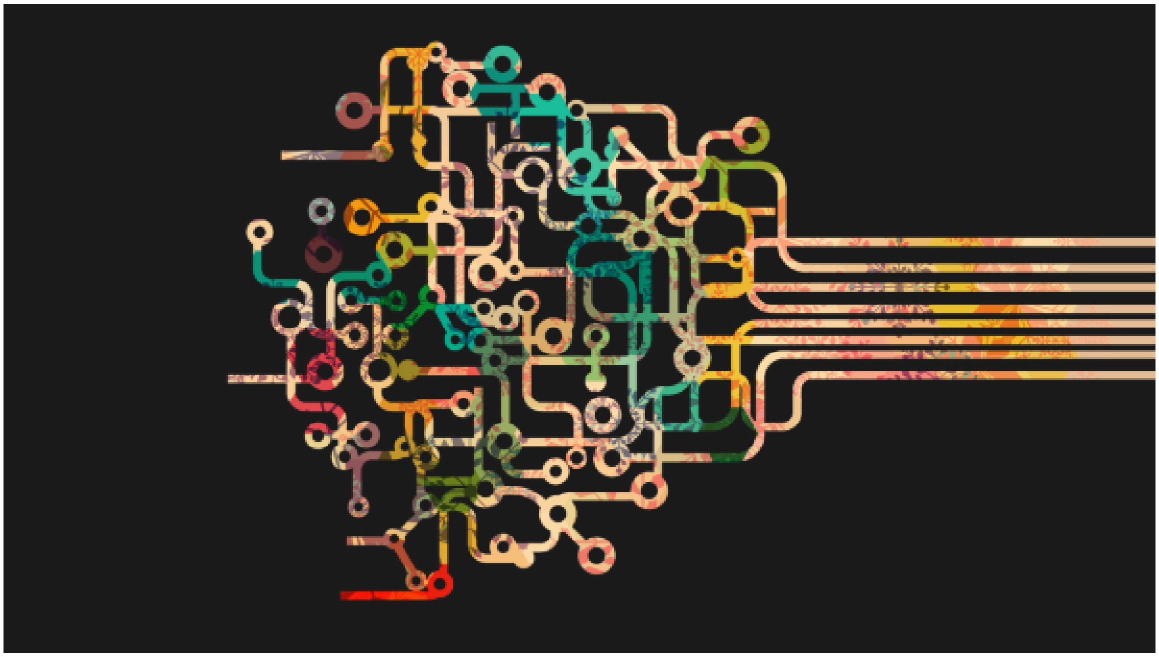
Harvard
Business
Review

RISK MANAGEMENT

More Training Won’t Reduce Your Cyber Risk

by Michael Sulmeyer and Mari Dugas

NOVEMBER 24, 2017



naqiewei/Getty Images

How many times have you had to watch your company’s latest cybersecurity training video? An entire industry now exists to train us humans to be smarter in how we operate computers, and yet the number of cybersecurity incidents continues to rise. Are the hackers always one step ahead? Are we impossible to train? Or are we being taught the wrong lessons?

The human is indeed the weakest link in cybersecurity. But all too often organizations' approach to mitigating that risk — other than taking the wise step of ensuring that they have the state-of-the art technological protection in place — is more training. It won't suffice.

The U.S. armed forces and security agencies are a case in point. Should the military train its soldiers, sailors, generals, and admirals so they are less of a weak link for cybersecurity, as Admiral Sandy Winnefeld, the former vice chairman of the U.S. Joint Chiefs of Staff, advises? Sure. Should the National Security Agency (NSA) do the same for its employees to keep secrets secret, as the *New York Times* indicates has been a challenge? Obviously.

But in truth, these parts of the U.S. government have been trying to make their workforces more cyber-savvy for years, and yet the hacks keep coming and succeeding — even against the U.S. military's Joint Staff network, which the *Washington Post* reports was compromised in August 2015 via a measly phishing e-mail. Putting them through 50 more hours of cyber-hygiene training a year won't help any more than warning our elders not to click on links in e-mails from strange addresses. We will never be able to train every e-mail recipient to discern what looks like a phish.

There is one area where more training would pay off: for CEOs and other senior managers — the people who are least likely to take training or take it seriously. Forty percent of respondents to a BAE Systems survey of senior managers in various sectors said they lack understanding of their own company's cybersecurity protocols. But if you're the boss, you're an attractive target for crooks and spies.

Most importantly, the training can help leaders be much more effective in overseeing chief information officers (CIOs), and chief information-security officers (CISOs). With training, leaders can make more informed tradeoffs between purchasing the most convenient, accessible, and affordable technology (the CIO role) and keeping that technology and a company's critical data secure (the CISO role).

When it comes to everyone else in the organization, however, the answer is not more training; it is to *not* trust humans in the first place. There are simply too many chances for us to accidentally hurt ourselves or the networks on which we operate regardless of how much training we receive. What we need to do is to help users and customers keep themselves and their households and organizations out of trouble.

The following proposals are all about companies' being proactive with strengthening the security of their own networks and computers. They will make a company and its users more secure, regardless of whether or not they receive more training.

Know and prioritize your information. It may be the most common cybersecurity advice out there (even White House cyber coordinator and former NSA chief hacker Rob Joyce says so!), but you are nowhere if you don't know your network and then prioritize what you need to defend. You can't defend what you don't know, and there's no way to defend every file, database, and folder equally. So leaders should invest the time in knowing their organization's network. It's the first necessary (albeit insufficient) step to help your humans do their jobs safely while keeping the bad actors out.

Don't let friends click links. In 2015, the U.S. Department of Defense (DoD) decided enough was it enough: to prevent its users from clicking on potentially malicious links, it converted all incoming mail from non .mil domains to plain text. Now, there are no links to click. Inconvenient? Perhaps. But this is a case where an enterprise decided the risks of convenience outweighed the rewards, and DoD leadership took action to keep its employees from causing inadvertent harm to the military's network.

Don't just share information; block it. Take advantage of services like Facebook's Threat Exchange that can feed threat information to perimeter defenses that can block attempts at malicious connections. This approach will never keep an enterprise perfectly safe, but it will reduce the risk of infection from those sources known to the community. And the unfortunate truth is that many, if not most, threats feature indicators that are known to various information security communities ahead of time.

Reduce your attack surface. Most of us at work use computers that have far too much capability than we need or use on a daily basis. With that capability comes increased risk due to all sorts of additional avenues of infection. If you can swing it, think about using something minimal like the entirely browser-based Chromebook, which can dramatically reduce the opportunities presented to an adversary or criminal to gain unauthorized access to your system. Its updates are far more regular and there is far less excess software to infect.

Reach for the cloud. Sophisticated businesses and enterprises are able to manage the security of their domain with a mix of security products. But many small and medium-size businesses don't have the resources to do so. Meanwhile, companies like Google spend millions on trying to keep hackers out of their e-mail infrastructure. If you are concerned you don't have the resources to manage your own e-mail security, consider switching your back-end e-mail infrastructure to Google's to take advantage of their investments in security. It spends a lot of time hunting hackers so you don't have to.

Finally, don't forget the insider threat. Cybersecurity professionals spend a lot of time keeping the bad guys out. But sometimes, good guys become bad guys. In fact, IBM estimates that 60% of all attacks are from the inside. A human-centric approach to limiting damage from insiders might include creating a culture of mutual accountability (some might say tattletaling) at work. Additional checks on insider threats include segmenting a network so that only those who need access to certain data get access to that data and "water-marking" sensitive data with information as to when and by whom it was accessed.

***

It would be silly to aim for or promise perfect security. Instead, these suggestions are meant to help reduce the risk of an attack. Not all will be appropriate for every situation or user, but together, they go a long way towards giving the human a hand to improve cybersecurity.

Michael Sulmeyer is the cyber security project director at the Belfer Center for Science and International Affairs at the Harvard Kennedy School. Previously, he served as the Director for Plans and Operations for Cyber Policy in the Office of the Secretary of Defense. Follow him on Twitter at @SultanOfCyber.

Mari Dugas is the project coordinator for the Cyber Security Project and Defending Digital Democracy at the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government.