# Overcoming 'cyber-fatigue' requires users to step up for security

January 24 2017, by Richard Forno

Credit: AI-generated image (disclaimer)

As a new presidential administration takes over, it will need to pay significant attention to cybersecurity. Indeed, we've already been told to expect "a comprehensive plan" for cybersecurity in the first few months of the new administration. But as a professional who has long been part of the global internet security community, I am pessimistic that the

typical government and individual plans or responses to our ongoing cybersecurity concerns actually will lead to meaningful improvements.

For decades, this cycle has repeated itself. First, a high-profile incident occurs – like the two massive Yahoo hacks revealed in 2016 or the even more damaging breach of federal employee data disclosed in 2015. Among other things, the resulting advice is the same: Users should change their passwords and make their login process more complicated (and more secure) by enabling two-factor authentication.

The affected services often require users to reset their passwords, but research shows very few people enable features like two-factor authentication. And even if they can, few people consider canceling their accounts – they depend too heavily on specific email addresses or other internet services in their daily lives.

Policymakers get stuck, too: New groups of well-heeled executives convene to study the same old problem and end up issuing the same old recommendations anyway. The cybersecurity industry remains a constant presence by offering new white papers, products and services to meet these many recurring challenges, too.

In broad terms, though, we do nothing at all. Over time, this leads to what I call "cyber fatigue" – namely, an inability to think critically about what needs to happen for meaningful, lasting cybersecurity improvements while focusing only on near-term problems. So as 2017 unfolds, instead of falling prey to cyber fatigue and tolerating the "status quo cyber," we should capitalize on the global trend toward radical change in taking some new approaches to internet security thinking. That includes how we as consumers and users of technology, both large and small, act to protect ourselves and our systems.

## Take serious steps toward real security

First and foremost, we must not merely address minor symptoms while ignoring the underlying disease. Transforming our information environment into a more resilient one will take concentrated time, money and even temporary disruption, all of which we must be willing to endure to achieve long-term benefits.

For example, we should not create new – and likely redundant – government organizations, policies or complex frameworks about internet security. Instead, we should reduce their numbers and complexity, giving the ones that remain more policy latitude to handle the rapidly varying security threats as they arise.

When new laws or regulations might affect the internet, like 2015's Open Internet Order, policymakers must ensure we all benefit – not just a select few companies or industries. They must treat the internet as a public resource and a public trust whose security and stability are not to be subverted to the service of private special interests.

As customers and users, when evaluating new technologies, systems, products and services, we must look beyond the attractive benefits, conveniences or cost savings they might offer. We must assess their potential risks, vulnerabilities, problems. And we must look at the possible consequences of embracing these items in our lives, workplaces and societies. Unfortunately, it's only after likely preventable problems occur that we consider the security issues associated with these technologies.

And above all, we need to move beyond offering policymakers' favorite plan, "information sharing," as some sort of solution to real-world issues. Yes, it's helpful, but the problem isn't how to better collect and share more information: It's how to better understand and act upon the information already collected.

## Move beyond technical 'cybersecurity education'

There is a global need for a larger and highly skilled cybersecurity workforce. Much of that will be hands-on practitioners performing technical or operational tasks. Accordingly, many efforts tend to focus on producing task-oriented technicians through intensive technical bootcamps, cyber competitions, or the misguided belief that everyone needs to be a "coder" to be a successful member of the technology workforce.

Protecting a network and the information stored on it is more than installing a security software package or technical prowess. It requires knowing how to build and modify them and understanding how they operate. To develop security policies and then assess why they do (or don't) work, one needs to understand psychology, sociology and other aspects of the human condition, and how to communicate effectively with people. Technology is so ingrained in modern life that analyzing its security issues exclusively from an engineering perspective, or treating it as something different or somehow removed from people and society, is folly.

Moreover, putting cybersecurity-related concerns into a real-world context requires an appreciation or understanding of the humanities and how people interact with technology as a whole, not simply competence in step-by-step technical procedures. Yes, we need people with solid technical skills, but that's only one, albeit important, aspect of a competent global cybersecurity workforce. In fact, changing our approach to cybersecurity means changing our mindset. Effective cybersecurity depends not just on technical fixes done by programmers but an appreciation that it is a shared responsibility of all users.

## Analyze information rationally and objectively

Building on the education theme, security professionals know that the most effective way of exploiting a system is by attacking the minds of its users and administrators. Called "social engineering," this type of attack is extremely successful because individual users' actions remain the most challenging cybersecurity problem.

Properly developed and deployed security technologies such as malware filters can make these attacks more difficult (but not impossible) to succeed. So can the implementation of more securely designed email systems and authentication protocols. But, since technology can go only so far, we must teach and reinforce basic technology literacy and digital citizenship at all levels of society. However, increasing technical literacy cannot occur in a vacuum or be based exclusively on technical concepts.

Yes, our education system must teach science, technology, engineering and mathematics to students. Humans are the weakest link in cybersecurity protection, which means that we must remain skeptical and security-minded whenever we're online. Courses in the humanities, history and rhetoric assist in developing the critical thinking skills and inquisitive minds needed in the modern workforce and nicely complement any necessary technical skills. Such lessons will better inform citizens, users and cybersecurity professionals alike.

So instead of repeating the same guidelines and recommendations of the past, it's time to take a new and unconventional look at our approach to technology and how we secure it. Certainly, many of our current best security practices still hold value. But unless we're willing to go beyond our traditional cybersecurity "comfort zone" and explore new solutions, our cyber-fatigue will worsen.

We know what needs to happen. What is required now is the courage and willingness to make it happen. Otherwise, the likely response from seasoned cybersecurity professionals following future cybersecurity

incidents will be to shake our heads and say, "We told you so."

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation