BEHAVIORAL scientist

TECHNOLOGY

Why Governments Should Treat Cybersecurity the Way They Do Infectious Diseases

By **Karen Renaud** and **Stephen Flowerday**
September 10, 2018

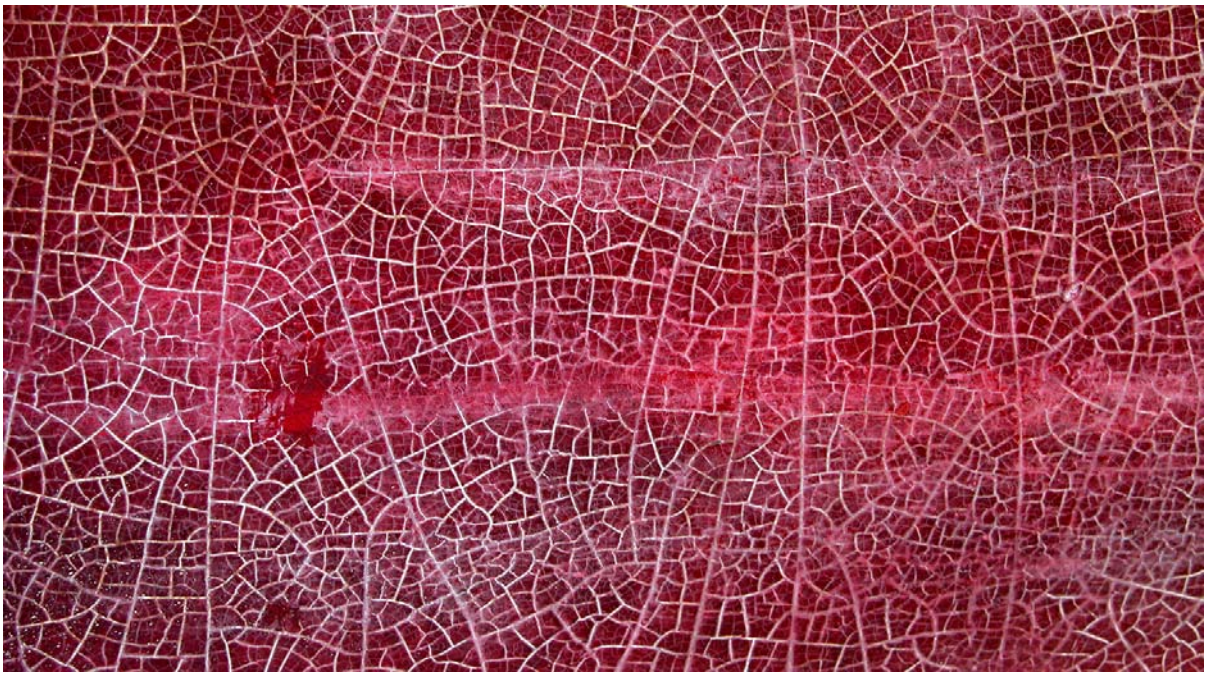


Image: Matt Artz/Unsplash

This article is part of our special issue "Nudge Turns 10," which explores the intersection of behavioral science and public policy. View the complete issue here.

Shelby first hears about the disease on Twitter. Journalists are saying that people in the small American town of Mayberry, just 10 miles from Shelby, are catching what they're now calling "Mayberry fever." It appears to be deadly.

Shelby is concerned, so he does an internet search for Mayberry fever vaccine. He finds a few online companies selling a vaccination, which they claim is 100 percent efficacious. He orders it and chooses overnight shipping. When it arrives, with the obligatory syringe and needle, the instructions are littered with

medical terminology and scary warnings. He is conflicted. If he does not vaccinate himself he might catch Mayberry fever. On the other hand, the vaccination itself might make him ill, or may not work at all. These vaccinations aren't regulated by the government, but people self-administer them anyway.

This scenario sounds ridiculous, doesn't it? Though Shelby and Mayberry fever are fictional, the reality is that we accept the responsibility to "vaccinate" ourselves when it comes to cybersecurity threats. For instance, if Shelby attempts to inoculate his own devices against a particular computer virus, he might still be vulnerable but blissfully unaware of it. If he takes the wrong measures, he could easily still fall victim to an attack. Shelby is not a doctor so cannot vaccinate himself against infectious diseases, nor would he likely know how to determine the efficacy and safety of a particular vaccine without some kind of regulating system. He is also not a cybersecurity specialist, so why is he expected to protect himself against cyberthreats, without any assistance?

Though a cyberattack may not lead to Shelby's demise, it still represents a serious threat. If he experiences a ransomware attack, he would have the choice either to pay the significant ransom or to lose all of his sensitive personal and other valuable information. If an identity thief steals his identity, recovery can take years. His close family could also be affected. A successful hack would not merely inconvenience Shelby but could also devastate his life and damage his career.

Cybersecurity attacks, like disease, have the potential to become calamitous and are contagious.

The answer may not be for Shelby to enroll in a cybersecurity course but rather for his government to take a more proactive approach in supporting its citizens in securing their devices. At the moment, many governments pass the burden of dealing with cybersecurity risks onto their citizens. Governments might offer advice and describe best practice—such as "use strong passwords" or "make backups"—but it's up to citizens either to follow such advice or to cope with the inevitable consequences without help or support. In the jargon of politics, this is referred to as "responsibilizing" citizens to cope with particular risks.

This hands-off strategy seems reasonable when an individual's unwise behaviors or bad fortune only affect him or herself, such as with unhealthy eating. It's a different matter when individual behaviors can harm entire communities or countries. When it comes to infectious fatal diseases, such as tuberculosis, governments provide vaccination services and sanatoria to isolate the infected. Governments should start treating cybersecurity as they do infectious diseases.

Cybersecurity attacks, like disease, have the potential to become calamitous and are contagious; we call the programs that infect our devices "viruses" for good reason. The WannaCry hacking attack crippled computers in 150 countries in May 2017, spreading from one to the other until it was deactivated by a "kill switch." Data that are stolen from one person's device via a successful hack are likely to include the personal details of many other people, potentially endangering the wider community. For example, Shelby will almost certainly store many friends' and contacts' mobile numbers and email addresses on his phone, and perhaps also their birthdates and other very personal details in archived email messages, all of which a successful hacker can access and possibly abuse.

In these cases, more advice is unlikely to increase security in a meaningful way. Even the advice that's out there is conflicting or so littered with techno-jargon that most people won't be able to understand it. On top of that, technology changes so fast, and new vulnerabilities emerge at such a rate, that any countermeasures Shelby takes might quickly become insufficient. All of this could lead to a troubling scenario: Shelby might feel confident that he's secure and yet still be vulnerable.

Hardly a day goes by without the media reporting yet another successful hack. Einstein said that continuing to do the same thing while expecting different results is insanity. The advice-only approach is clearly not working, so we should think about another strategy.

It is time for governments to rethink the way they support citizens' cybersecurity.

It is time for governments to rethink the way they support citizens' cybersecurity—and how behavioral science can play a role in making all of our devices more secure. New York is already moving in this direction.

For example, when a widespread attack occurs, governments could instruct citizens, in a specially-crafted text message, to implement specific countermeasures on all their devices to stop the attack from spreading. Such a countermeasure could be emergency installation of an update to render the malware ineffective. To increase uptake, governments could design their text messages with human behavioral principles in mind. They could, for instance, highlight the number of other people who have already downloaded and installed the update, and send the text message in the hour after a TV news report on the attack. Governments may want to collaborate with mobile-phone manufacturers to bundle interventions as verified updates. This way, hackers cannot masquerade as government agents and send fake text messages to direct people to hacker-owned websites.

Cybersecurity is in its infancy when we compare it to more established fields such as health care. We cannot afford to wait for risk management strategies in this field to mature at the same pace that has characterized developments in more established fields. Instead, we should use strategies that have proven effective in other domains. Only in this way can governments help people like Shelby to foil those who seek to benefit from the general public's unsecured devices.

Karen Renaud

Karen Renaud is a professor of cyber security in the Division of Cyber Security at the University of Abertay in Dundee, Scotland. She holds a first class masters degree in computer science from the University of South Africa, and a Ph.D. from the University of Glasgow.

Website

Stephen Flowerday

Stephen Flowerday is an NRF-rated researcher in South Africa. His research focuses on cybersecurity, behavioral information security, and information security

management. He holds and MBA and a Ph.D. in information technology.

Website

Further Reading & Resources

- Leyden, J. (2018). Schneier warns of 'perfect storm': Tech is becoming autonomous, and security is garbage. *The Register*. (Link)
- Gray, G. C. (2009). The responsibilization strategy of health and safety: Neo-liberalism and the reconfiguration of individual responsibility for risk. The British Journal of Criminology, 49(3), 326-342. (Link)
- Hatmaker, T. (2018). New York City is launching public cybersecurity tools to keep residents from getting hacked. *Tech Crunch*. (Link)
- Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious?. *Computers & Security, 78*, 198-211. (Link)
- Behavioral Insights Team. (2014). *EAST: Four simple ways to apply behavioural insights.* (Link)

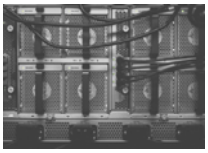
CYBERSECURITY GOVERNMENT POLICY

RECOMMENDED FOR YOU

TECHNOLOGY

What's True, and Fake, About the Facebook Effect

By **Jessica Feezell** and **Yanna Krupnikov**



TECHNOLOGY

The Road to Cybersecurity Is Paved With "Extraordinarily Basic Things"

By **Gregory Michaelidis**

TECHNOLOGY

The Real Reason You Shouldn't Text While Driving

By **Aline Holzwarth**