8 Cybersecurity Predictions for 2019

from LogRhythm Labs

A cyberattack on an automobile will kill someone.

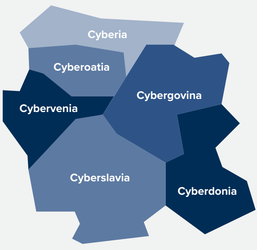
We've already seen hackers remotely kill a Jeep on the highway, disable safety features like air bags and antilock brakes, and hack into a car's Bluetooth and OnStar features. As cars become more connected and driverless cars evolve, hackers will have more opportunities to do real harm.

Cybersecurity programs will grow but continue to lag behind the talent gap's growth by at least 25 percent.

The Bureau of Labor Statistics anticipates available jobs for information security analysts will grow 28 percent between 2016 and 2026.[1] But since 2014, only 3.7 percent of American universities and colleges have met the requirements necessary to be recognized by the National Centers of Academic Excellence in Cyber Defense Education Program (CAE-CDE). Unfortunately, we don't expect the acceptance rate to suddenly increase, meaning cybersecurity program growth will lag behind the talent gap by at least 25 percent in the coming year.

Bio-identifiers will outpace traditional passwords.

Authentication using biometrics – especially facial recognition – continues to grow in popularity, and we don't see this slowing down any time soon. Case in point: Apple didn't simply just add Face ID capabilities starting with the iPhone X; it completely swapped out Touch ID for the latest biometric trend. As ease of use remains a top priority for users, we'll see traditional passwords decline in popularity.

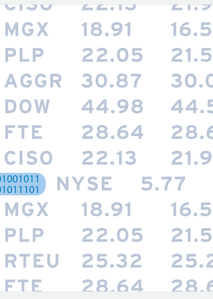


The United States will experience the "balkanization" of cybersecurity regulations.

The United States has been slow to enact cybersecurity legislation at the federal level. As a result, states have started taking matters into their own hands. In 2019, we expect an increase in cybersecurity legislation at the state level. And given the lack of consistency among resulting regulations, this will lead to greater challenges when it comes to interstate business operations.

China will manipulate the market to turn the trade wars in their favor.

China isn't new to cyberespionage, with reports revealing their efforts cost the United States upwards of $300 billion annually.[2] The United States reacted earlier this year by imposing a $50 billion tariff on Chinese imports. Given the economic impact of these tariffs, we expect China to leverage its cyber-spies to give itself an advantage in the growing trade wars.



Cloud-based ransomware will compromise a major corporation's infrastructure.

Ransomware continues to grow in sophistication. In 2019, we believe we will see it successfully compromise a major corporation's cloud infrastructure. The results will be devastating, impacting thousands of customers and resulting in a heavy loss of profits due to missed SLAs and fines.

We'll see a move to hold CEOs accountable for breaches.

There are already regulations to hold people accountable (notably CISOs) for breaches. But as the pace and damage of breaches become more severe, we believe we'll see these regulations begin to expand accountability to the CEO role.

Trump's cell phone will be hacked.

Yes, we've said this one before, but with the President using an unencrypted phone to communicate with leaders of nations, this has to be a hot target. Just imagine what the potential impact will be — not to mention what we'll see on Twitter.

Curious to see how our past predictions have held up?

View them here.

LogRhythm Labs is a dedicated team within LogRhythm that delivers security research, analytics, and threat intelligence services to enable your security operations center and protect your organization from damaging cyberthreats.

1. Improving Cyber Defense Education through National Standard Alignment: Case Studies, IGI Global, Jan. 1, 2018 // 2. China's Cyber Espionage Continues, and There's a Big Cost, Alliance for American Manufacturing, Sept. 6, 2018

LogRhythm Labs