Information Security Predictions for 2017

from the LogRhythm Labs team

1 There will be an overt cyber attack from a nation-state.

The public nature of this action will force the hand of NATO, the UN, or the U.S. government to retaliate —whether they choose to do so remains to be seen.

This will lead to an increased focus on offensive cyber capabilities and will bolster the demand for cyber weapons. Countries with limited capabilities might choose to purchase cyber weapons on the black market. Countries could covertly arm their allies with cyber weapons and encourage disguised attacks on their enemy.

2 The internet will be shut down for up to 24 hours.

In 2016, we saw DDoS attacks against a major DNS service provider that knocked down a large portion of the U.S. internet.

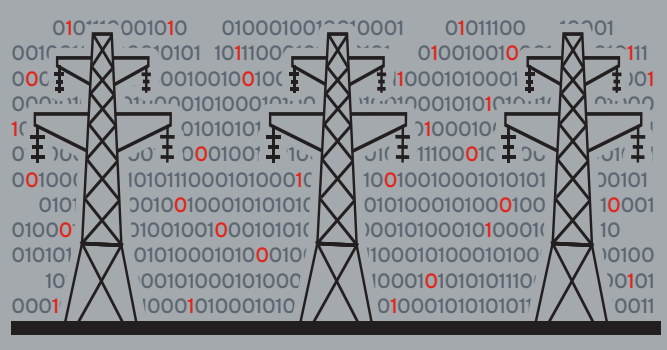
We know there have been critical vulnerabilities in the fabrics that power the internet, and there are critical vulnerabilities not yet disclosed. We also know of nation-state threat actors who would use these vulnerabilities as potential cyber weapons.

Combine this increasing threat with our continued reliance on cloud-based services, and any internet outage could have significant financial ramifications for businesses.

3 Portions of the U.S. power grid will be shut down.

Critical infrastructure is a target for nation-state threat actors. Our infrastructure networks are becoming increasingly connected through IoT and internet-aware sensors.

With this new-found connectivity, an attacker could compromise the critical infrastructure directly or by using their network and devices to attack others.



4 The use of fake news and psychological warfare in the media will rise.

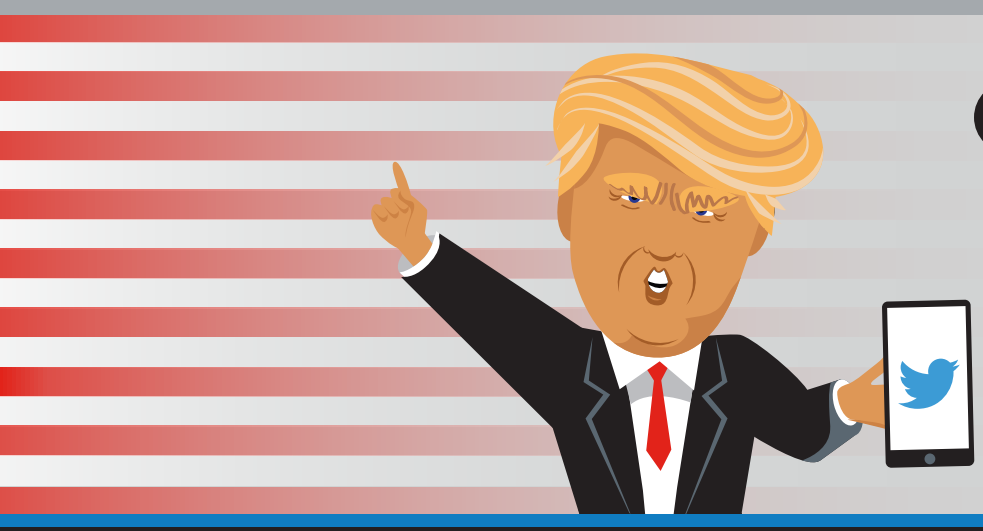
In 2016, we saw the rise of fake news and the use of social media as a vehicle for delivery—quickly causing the public to question the legitimacy of news sources.

We also saw major media outlets using psychological operations (PSYOPS) techniques during the U.S. election to sway public opinion.

As the battle between legitimate and fake news continues to heat up in 2017, we fully expect some level of retaliation that could lead to a major media outlet being taken offline.

5 Ransomware gets more personal with the rise of mobile ransomware.

Attackers will leverage ransomware to target personal and mobile computing devices. For example, attackers could hold incriminating photos or information from a politician, a celebrity, or any individual with a high valued personal brand until a ransom is paid.



6 President Trump's Twitter account will be hacked.

President Trump's personal Twitter account is too easy and enticing of a target for it not to be hacked. Hacking accounts on Twitter is a pretty frequent occurrence. What better way to damage the credibility of the President of the United States of America than to break into and use his own mouthpiece against him?

LogRhythm® Labs