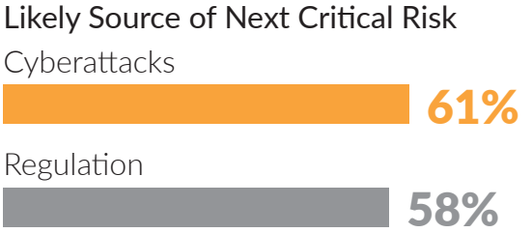
# 2017 PREDICTIONS
# CYBER REGULATIONS

Dan Lohrmann, CSO, Security Mentor

## DID YOU KNOW?

In the 2016 Retail Compass Survey of CFOs, nearly **7 in 10 retail CFOs** said they expected cyber regulation to grow in 2016.




The 13th Annual Excellence in Risk Management Report found that **61% of respondents cited cyberattacks** as the likely source of their organization's next critical risk. This was followed by regulation, cited by 58% of the respondents.

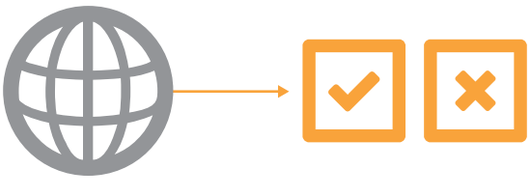
## PREDICTIONS: SURE THINGS

**Cyber insurance for data breaches will become required** to obtain certain government contracts in the United States. While this is sometimes true now, it will become more widespread. Also, insurance companies will start requiring effective end user security training as a requirement. This will be similar to Payment Card Industry (PCI) required end user training.

Internet of Things devices will become subject to some type of **federal government certification process** similar to how the federal government uses FedRAMP to evaluate cloud security. However, exemptions will render the regulations almost meaningless, since so many exceptions will be made due to volume of requests.

## PREDICTIONS: LONG SHOTS

A hacked automobile computer will cause a fatal car accident leading to lawsuits and a pause in autonomous vehicle deployment. This will bring more calls for **regulating autonomous vehicles.** The new U.S. presidential administration will initially resist regulations under pressure from technology companies, but will eventually support after similar incidents occur.



The continued growth in nation-state hacking and evolving cyber arms race will lead to the United Nations trying to issue **global regulations in cyberspace.** The U.S. government and others will veto these ideas—despite a heated public debate.