Information Security Predictions for 2018

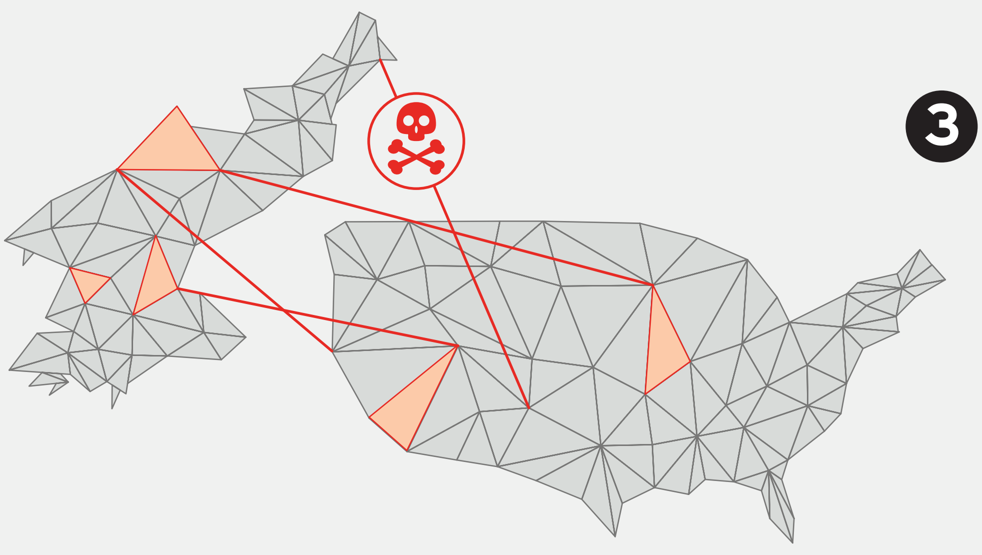
from the LogRhythm Labs team

1 A new record for the largest data breach settlement will be set.

Anthem currently holds the record at $115 million over a 2015 cyberattack that compromised data on 78.8 million people.

2 New U.S. legislation will be introduced to regulate activities related to privacy data and protection.

The U.S. government will introduce new legislation (similar to GDPR) around privacy data protection that will mandate how companies must protect privacy data information.

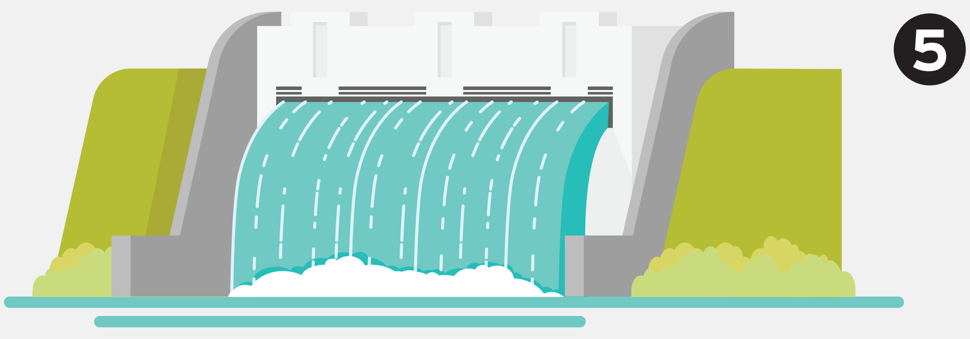


3 Cyberwar campaigns between North Korea and the US will emerge from the shadows and directly impact the public.

The U.S. and North Korea have been covertly carrying out cyberattacks against each other for years and ramping up their digital aggression. Tensions will continue to escalate, and the public will be impacted for the first time.

4 IoT devices will become a more frequent target for Ransomware attacks and cyber extortion.

Ransomware will continue to be a popular hacking method. Hackers will expand into new vectors and targets, impacting the everyday use of IoT.

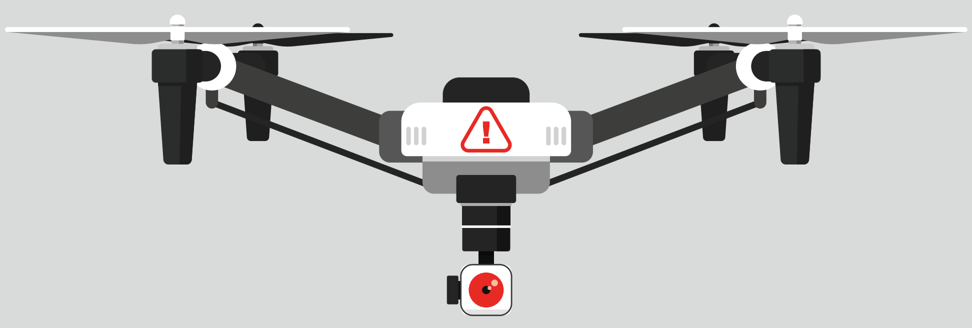


5 DDoSaaS will become a 'thing' and will result in another major DDoS attack against critical infrastructure.

Hackers will use a cloud service provider, such as AWS, to administer a DDoS attack.

6 Drones will be exploited much more often as a cybersecurity threat vector.

Despite existing restrictions to mandate no-fly zones, drones (like iPhones) can and will be "jailbroken." Expect to see quite a few cases where drones are used for more than just fun.



7 Bitcoin wallet exploits will result in massive losses of personal wealth.

Due to the increasing popularity of BTC, many individuals will have their BTC wallets hacked and potentially lose a lot of money--or worse, their life savings.

8 Kim Jung Un's PlayStation® account will be hacked.

LogRhythm® Labs