



# 2017 Threats Predictions

McAfee Labs

Intel Security shares predictions about the evolution of threats in 2017.

## Ransomware

Ransomware will peak in the middle of next year but then begin to recede.

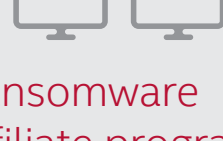
Ransomware advances in 2016



Ransomware attacks on IoT devices



Off-the-shelf ransomware



Ransomware affiliate programs



Ransomware-as-a-service

Total ransomware has grown 80% in 2016.

Ransomware source code

The security industry fights back to slow ransomware

Law enforcement actions

Anti-ransomware technologies



WildFire ransomware takedown



Malicious encryption detections



Shade ransomware takedown



Behavioral monitoring technology



Collaboration

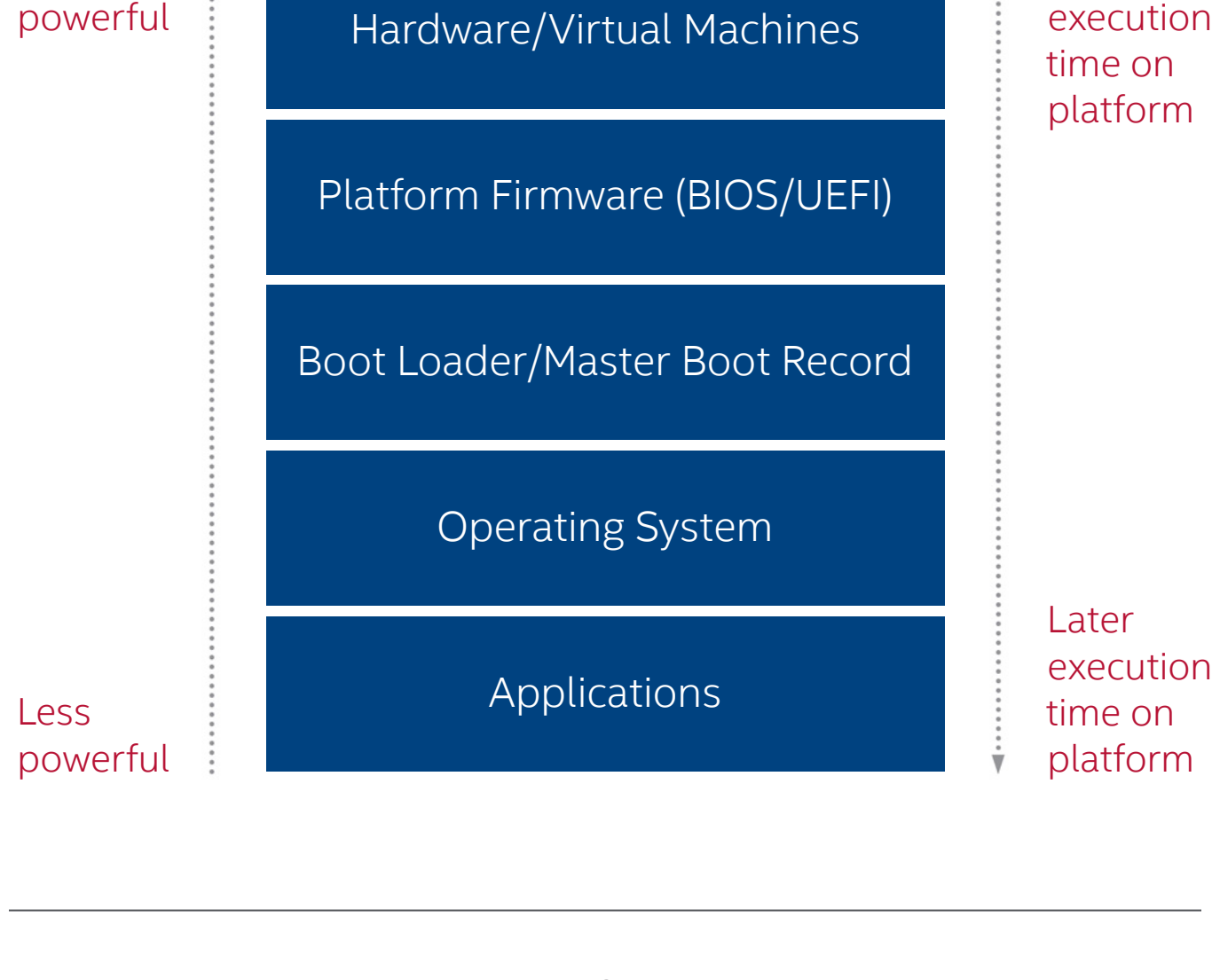
NO MORE RANSOM!



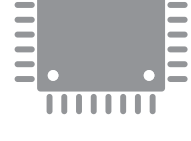
## Hardware Attacks

In 2017, we will see hardware attacks, system firmware attacks, and attacks on virtual machines.

Successful hardware and firmware attacks are more powerful than attacks on applications.



Known hardware and firmware vulnerabilities



Microprocessors



DRAM



Virtual machines



System firmware



Hard drives



USB devices



Network cards



Home routers



Printers

## Social Engineering Attacks

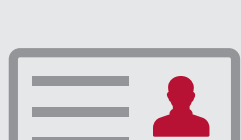
Machine learning will accelerate social engineering attacks.



Data exposed in 2016 for machine learning training



Medical records



Customer records



Email and social media records



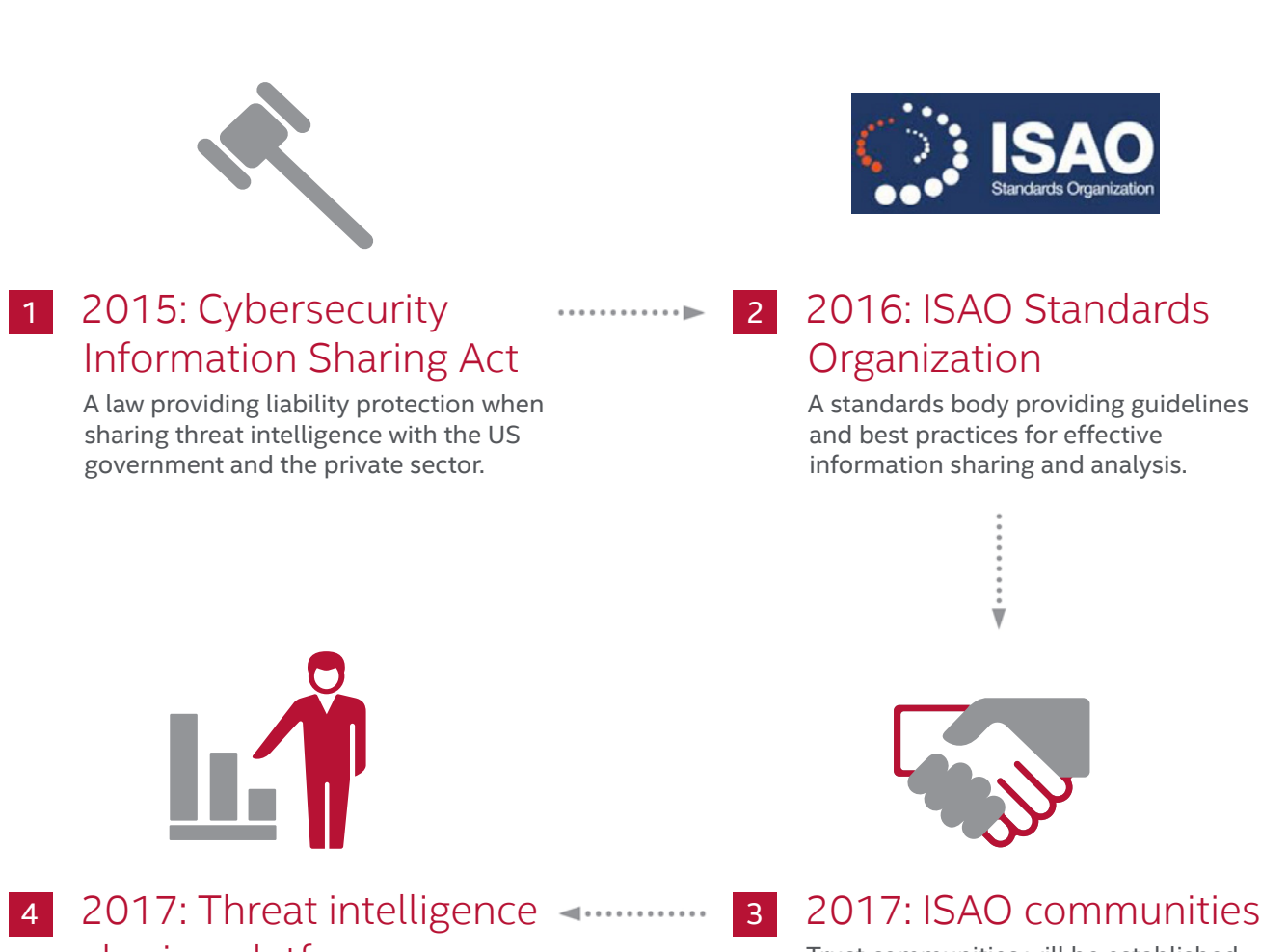
Business financial filings



Stolen data warehouses

## Threat Intelligence Sharing

Threat intelligence sharing will see major advancements in 2017.



McAfee Labs 2017 Threats Predictions

Visit [www.mcafee.com/2017Predictions](http://www.mcafee.com/2017Predictions) for the full report.

