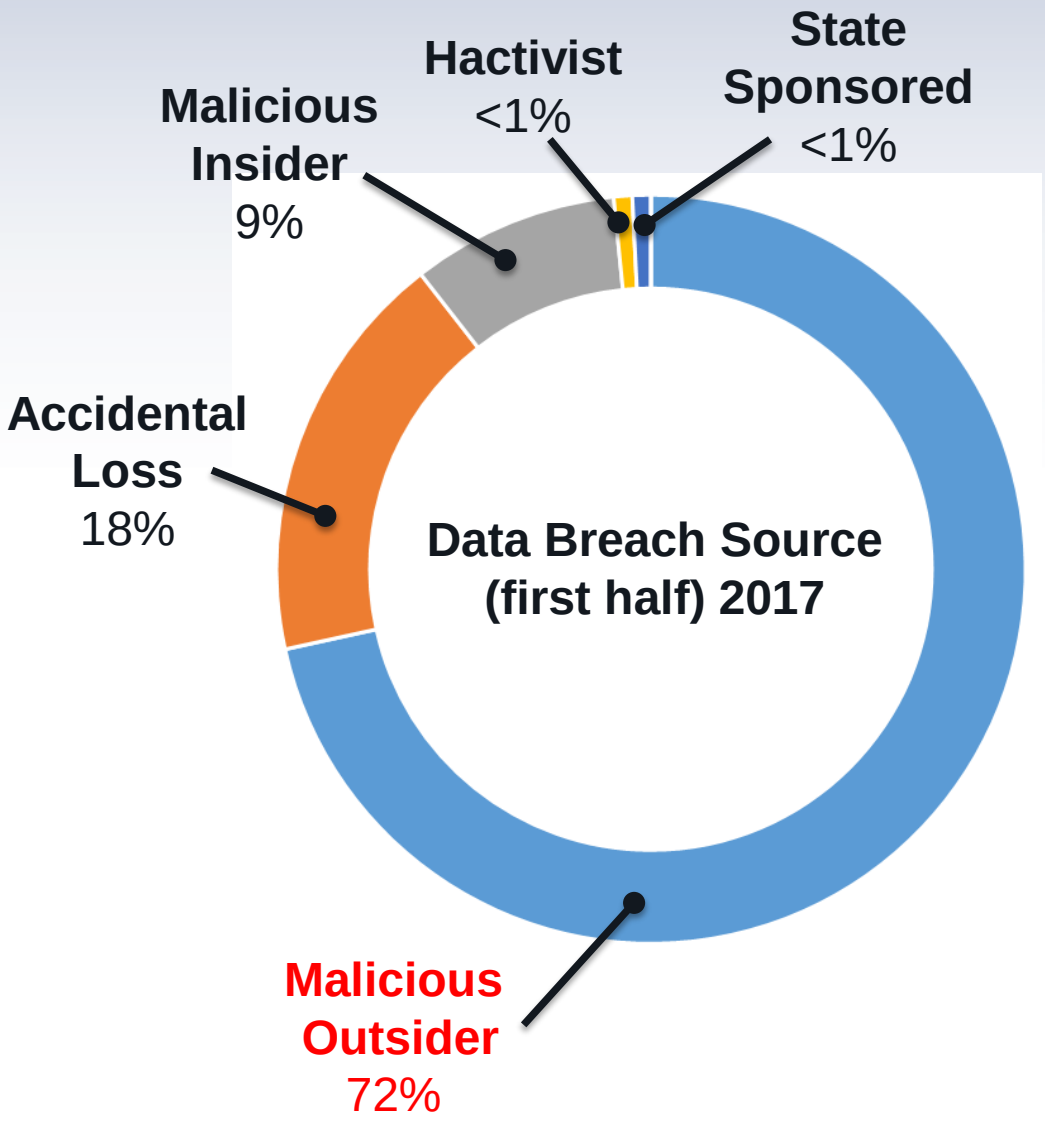
CyberHawaii

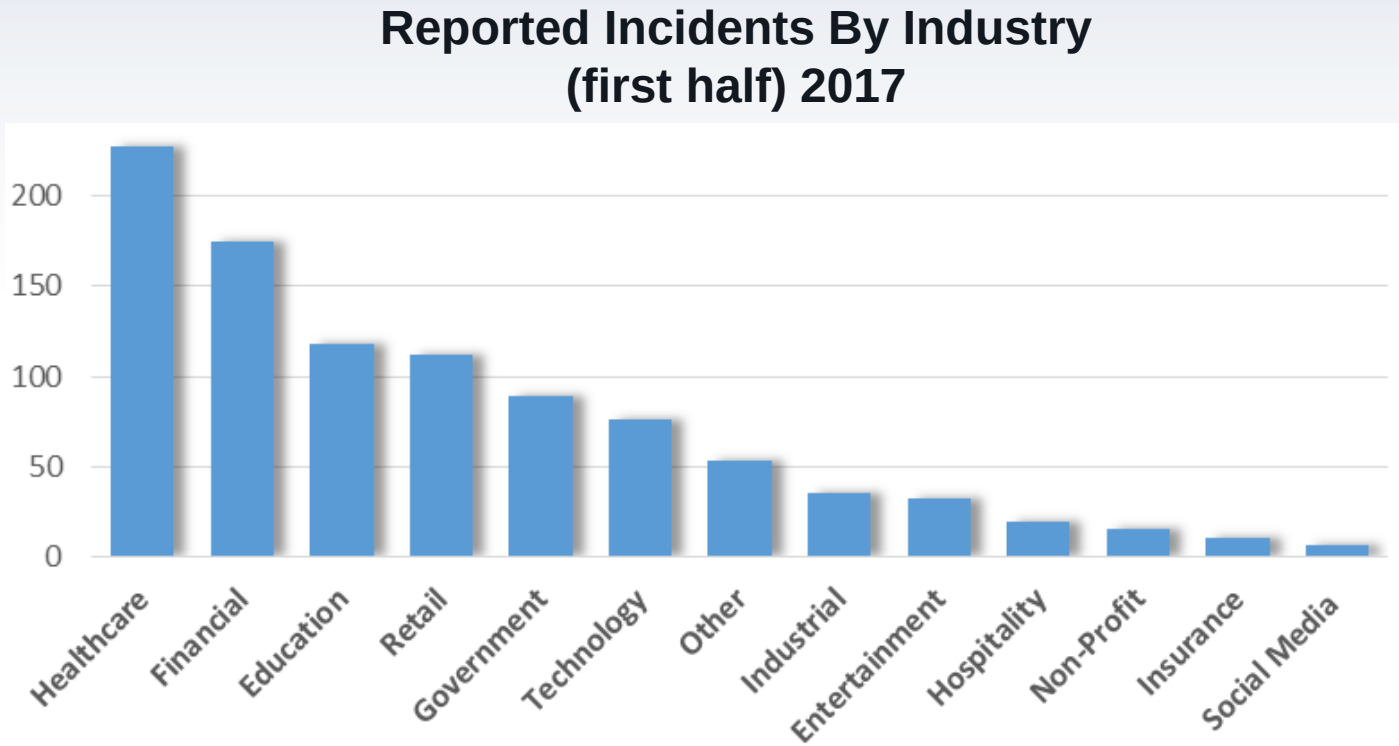
Cybersecurity is the Future of Computing

Dr. Robert J. Runser,
Technical Director, NSA-Hawaii

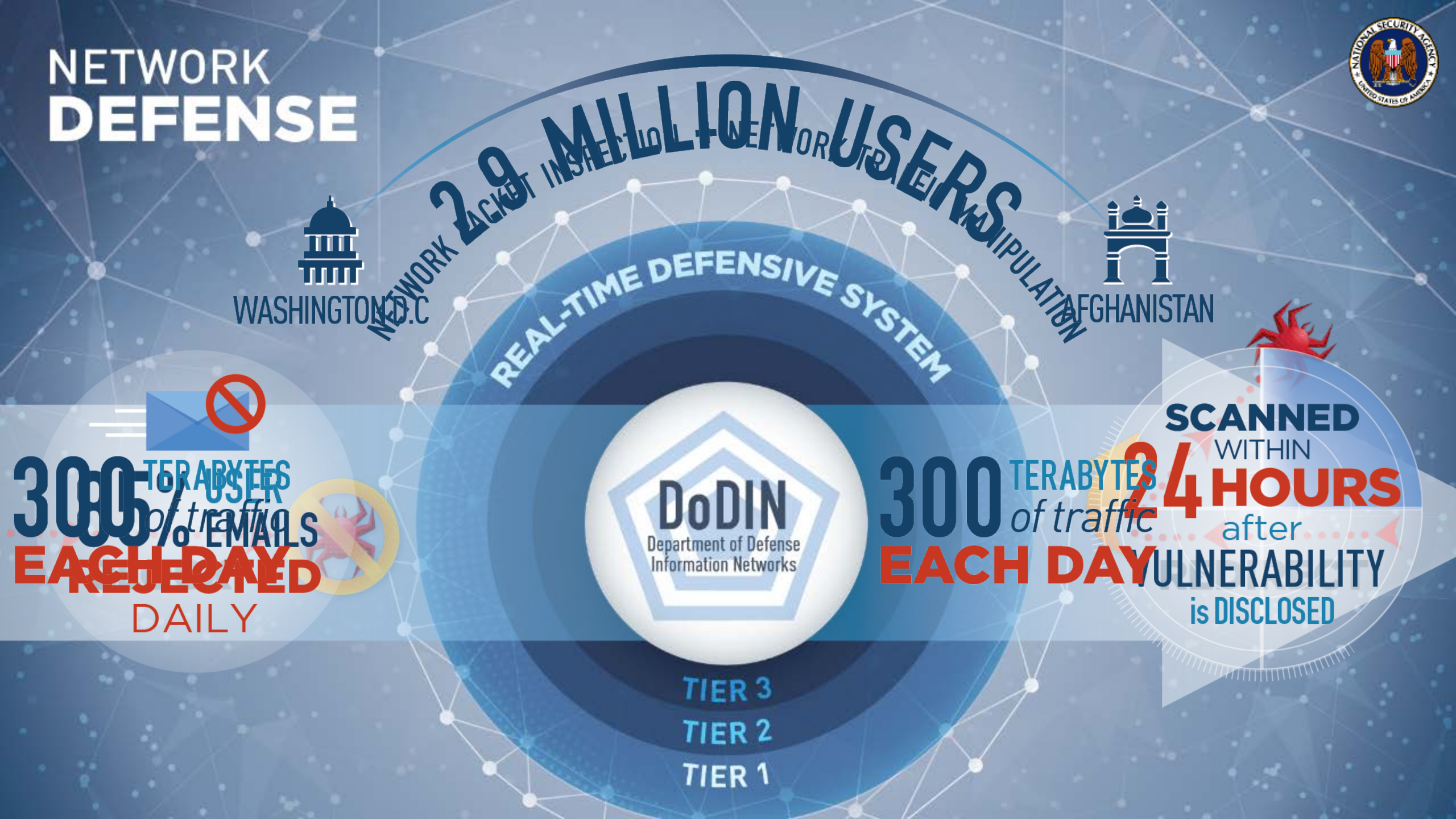
Data Breaches (first half) 2017

Source: http://breachlevelindex.com





NETWORK DEFENSE



CYBER THREATS

THE NEW NORMAL

CONTINUOUS TECHNIQUES TO OVERCOME DEFENSIVE MEASURES

'LEGITIMATE' CREDENTIALS OR SERVICES RATHER THAN RELYING ON TRADITIONAL MALWARE

AGGRESSIVE & DISRUPTIVE CYBER OPERATIONS

RAPID WEAPONIZATION OF DISCLOSED EXPLOITS

FREQUENCY OF AGGRESSIVE & ESCALATORY DISRUPTIVE CYBER BEHAVIOR

IN THE LAST YEAR ALONE, MULTIPLE DATA DESTRUCTION & RANSOMWARE CAMPAIGNS

Five Security Best Practices

NCTOC Security Operations Center Principles

https://www.nsa.gov/resources/cybersecurity-professionals/assets/files/top-5-soc-principles.pdf

1) Establish a Defendable Perimeter

2) Ensure Visibility Across the Network

3) Harden to Best Practices

4) Use Threat Intelligence & Machine Learning

5) Create a Culture of Curiosity

NSA Open Source Software Library

https://code.nsa.gov/

Guides and Tools for Cybersecurity

Windows-Event-Log-Messages

Retrieves the definitions of Windows Event Log messages embedded in Windows binaries and provides them in discoverable formats. #nsacyber

Windows-Secure-Host-Baseline

Configuration guidance for implementing the Windows 10 and Windows Server 2016 DoD Secure Host Baseline settings. #nsacyber

Spectre-and-Meltdown-Guidance

Guidance for the Spectre and Meltdown vulnerabilities. #nsacybe

Event-Forwarding-Guidance

Configuration guidance for implementing collection of security relevant Windows Event Log events by using Windows Event Forwarding. #nsacybe

unfetter

Identifies defensive gaps in security posture by leveraging Mitre's ATT&CK framework. #nsacyber

WHAT CAN WE DO?

MISSING
OPPORTUNITIES
TO **COLLABORATE**

INNOVATIVE
APPROACHES
TO **SECURITY**

OVERCOME ALERT
FATIGUE TO **PRIORITIZE**
RESPONSE **ACTIONS**