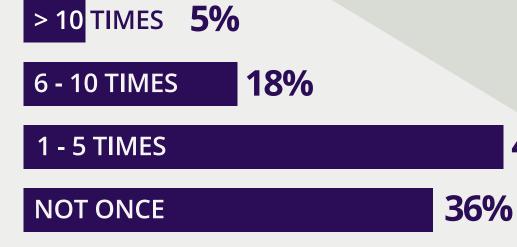


# 2016 CYBERTHREAT DEFENSE REPORT FOR GOVERNMENT AGENCIES

## **SURVEY DEMOGRAPHICS** > 25K 500 - 999 10K - 25K 1K - 4,999 5K - 9,999 6.4% Government **INDUSTRY COMPANY SIZE** (# of employees) Admin/Operations Architext/ Engineer Other Senior Mgmt. Analyst/Auditor **ROLES**

#### **GOVERNMENT UNDER FIRE**

The frequency of successful attacks against government agencies in 2015.



#### **CAUSE FOR CONCERN**

Only 21% are confident regarding the ability to monitor privileged users



41%

### **INCREASING SECURITY BUDGETS** With only 61% having their IT security budgets increase in 2016, government agencies are behind the curve in this regard. **TELECOM & TECHNOLOGY** 82% 77% **MANUFACTURING** 77% **FINANCE** 77% **HEALTH CARE** 71% **RETAIL GOVERNMENT** 61% 58% **EDUCATION**

#### CYBERTHREAT HEADACHES

Cyberthreats of greatest concern include...





threats



phishing attacks



#### **INADEQUATE ENDPOINT DEFENSES**

75% are evaluating new solutions to augment or replace their existing endpoint defenses.



## DOWNLOAD THE FULL REPORT AT: www.imperva.com/go/cdr

#### SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...





Low security awareness among employees

Too much data to analyze

#### **APPLICATION & DATA SECURITY DEPLOYMENTS**

The most commonly used technologies for securing applications and data include...







Web application firewall

#### **NETWORK SECURITY ACQUISITIONS**

The top four network security technologies targeted for acquisition in 2016 are...

firewall (NGFW)





service



