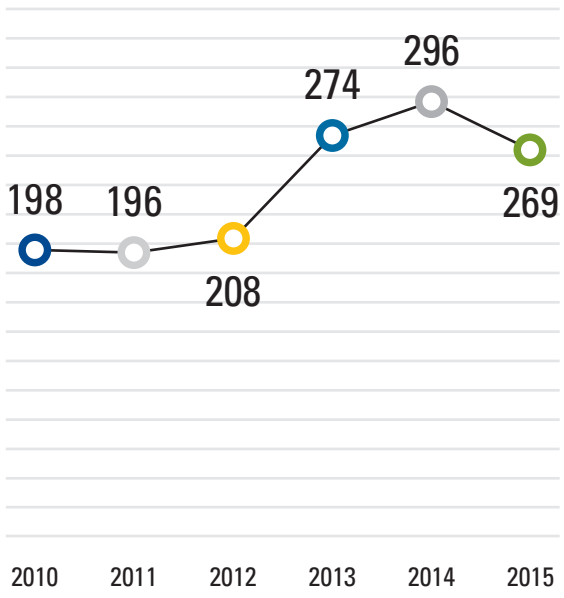
Spectrum ENTERPRISE | Navisite®

# The Healthcare Security Challenge

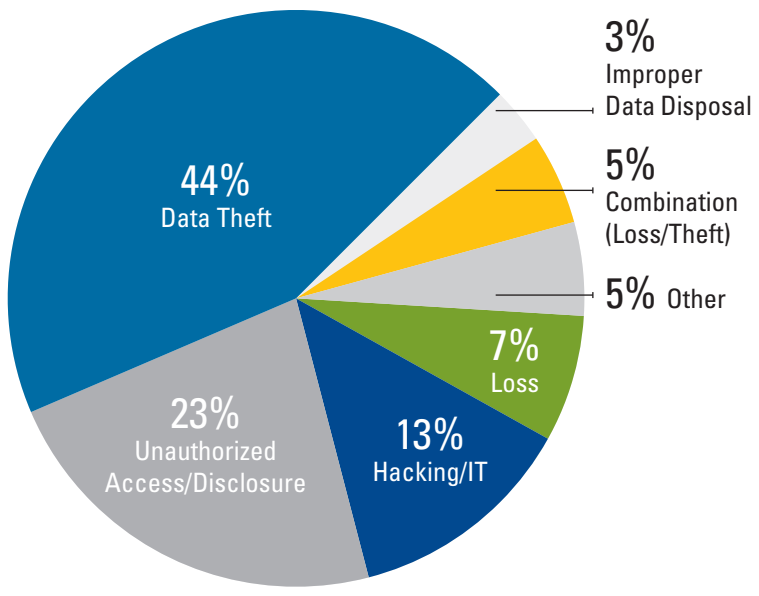
## THE SECURITY PROBLEM IN HEALTHCARE[1] 2009-2017

1625 Incidents | 159.5 Million Individuals

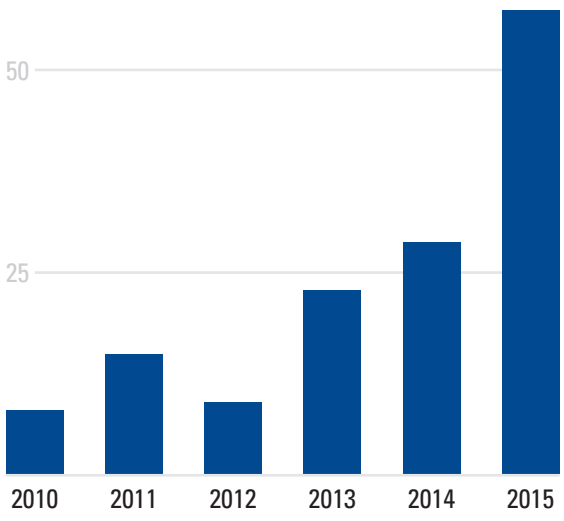
## GROWTH IN NUMBER OF SECURITY INCIDENTS




## BREAKDOWN OF SECURITY INCIDENTS IN HEALTHCARE




## HACKING/IT INCIDENTS IN HEALTHCARE GROW 286%

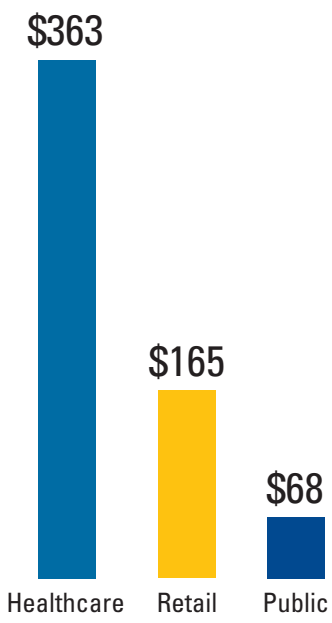



## ANNUAL COST OF HEALTHCARE SECURITY BREACHES[2]

$6 Billion

Includes remediation, legal fees, fines etc.

## HEALTHCARE RECORDS MOST EXPENSIVE




Average cost of security breaches per exposed personally identifiable record

## WHERE SECURITY PROBLEMS OCCUR


# THE 7 STEPS TO Developing a Healthcare Security Plan

### STEP 1
## REVIEW ORGANIZATIONAL GOALS

Get input from across the organization—the broader the input, the more the final security plan will truly align with and support organizational goals.

### STEP 2
## DEVELOP A RISK MANAGEMENT PROGRAM

Develop a risk management program to reduce overall exposure, prioritize resources and support long-term care-delivery strategies.

### STEP 3
## SUPPORT ORGANIZATIONAL OBJECTIVES

Detail a security plan that addresses key objectives and drives adherence to compliance programs, technologies and processes. Identify specific results to be achieved.

### STEP 4
## DETAIL POLICIES, PROCEDURES AND STANDARDS

Develop guidelines (policies, procedures and standards) to ensure that all compliance measures are identified and that the entire organization is advancing toward the same objectives.

### STEP 5
## ESTABLISH SUPPORT AND ALIGNMENT

Ensure that security plans are aligned with larger organizational goals AND the goals of the major departments that will be implementing them.

### STEP 6
## AUDIT AND REVIEW

Monitor your security plan on a regular basis to get reports on achievements and compliance levels and to maintain best practices. A third-party audit can provide an impartial review.

**To read more about each of the 7 steps, download this white paper: bit.ly/2bfvy0y**

### STEP 7
## COMMIT TO CONTINUOUS IMPROVEMENT

A commitment to continuous improvement is essential. Organizations should consider reviewing security policies at least every six months.

[1] Information on incidents, individuals and organizations impacted by security breaches are based on data reported to the Department of Health and Human Services since 2009 involving breaches affecting more than 500 individuals.

[2] Data on cost of healthcare breaches based on studies by Ponemon Institute: "Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study." Retrieved from http://www.ponemon.org/news-2/66