Streamlining Vendor Management with HITRUST®

Deana D Fuller & Gina Yacone

Agio, LLC

HIMSS NORTH CAROLINA *Chapter*

Intros

- Deana D Fuller, JD, CIPP/E, CPHIMS, CCSFP
- Gina Yacone, SSCP, CCFSP

- *DISCLAIMER: Nothing in this presentation should be interpreted as legal advice. This information is not intended to substitute for professional legal advice and does not create an attorney-client relationship. You should accept legal advice only from a licensed legal professional with whom you have an attorney-client relationship. You should contact a lawyer in your area, to assist you in any of these matters.*

Learning Objectives

- Understand the threat that third parties pose, and through examination of recent data breaches, learn how an effective vendor risk management program could mitigate that risk
- Learn the key components of an effective vendor risk management program and how HITRUST can provide them with a consistent method for managing vendor risk.
- Understand the HITRUST CSF Certification process, from both the Assessor and the Vendor perspective

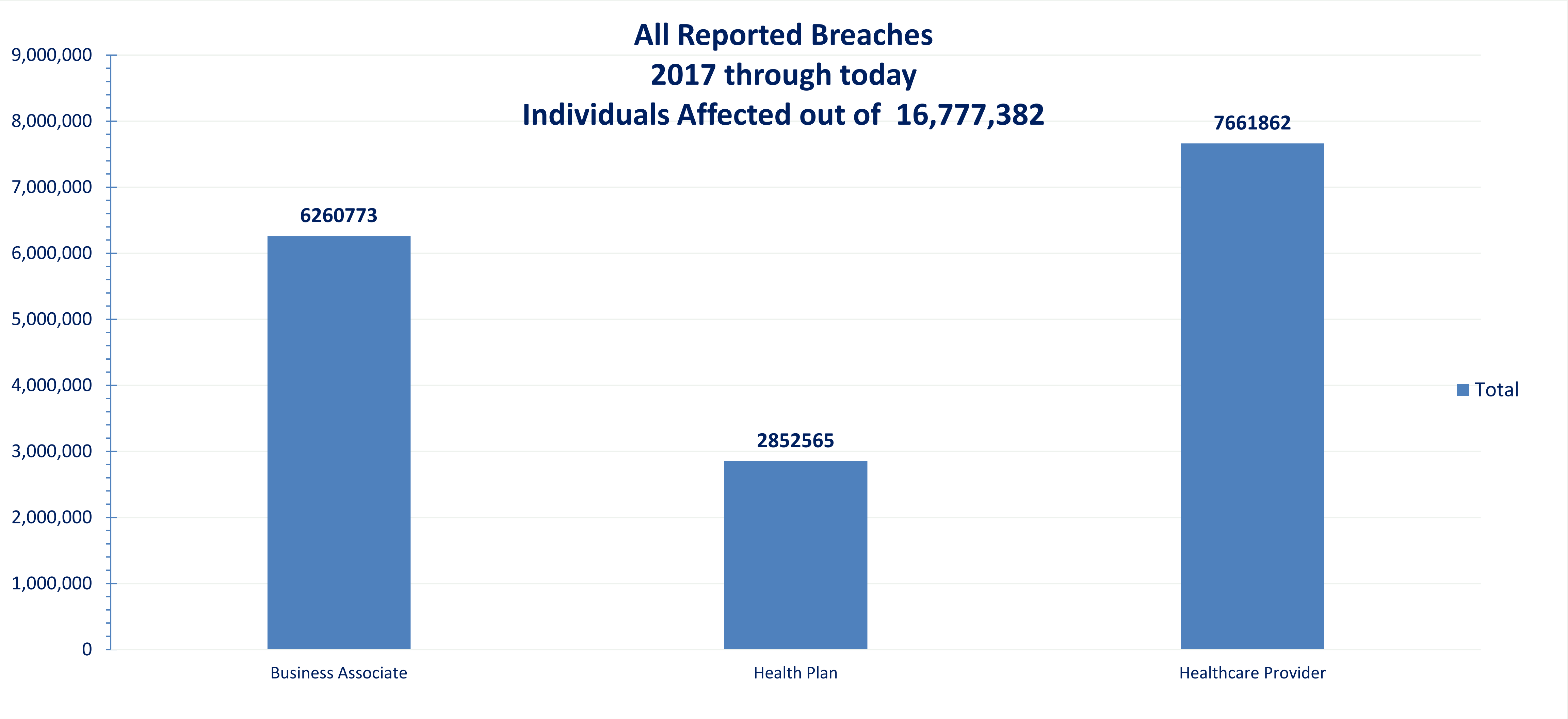
Overview

- Who cares?
  - You! Use a VRMP & HITRUST CSF Certification to simplify and ease your workload.
- What do you need?
  - Elements of a Vendor Risk Management Program
- When should we implement a VRMP?
  - Yesterday.
  - IoMT + motivated hackers + increased regulation = more cost when you have a data breach
- Why should you care?
  - Blind reliance on vendors causes recent data breaches
- How should a VRMP be structured?
  - The HITRUST CFS

Reliance on Vendors

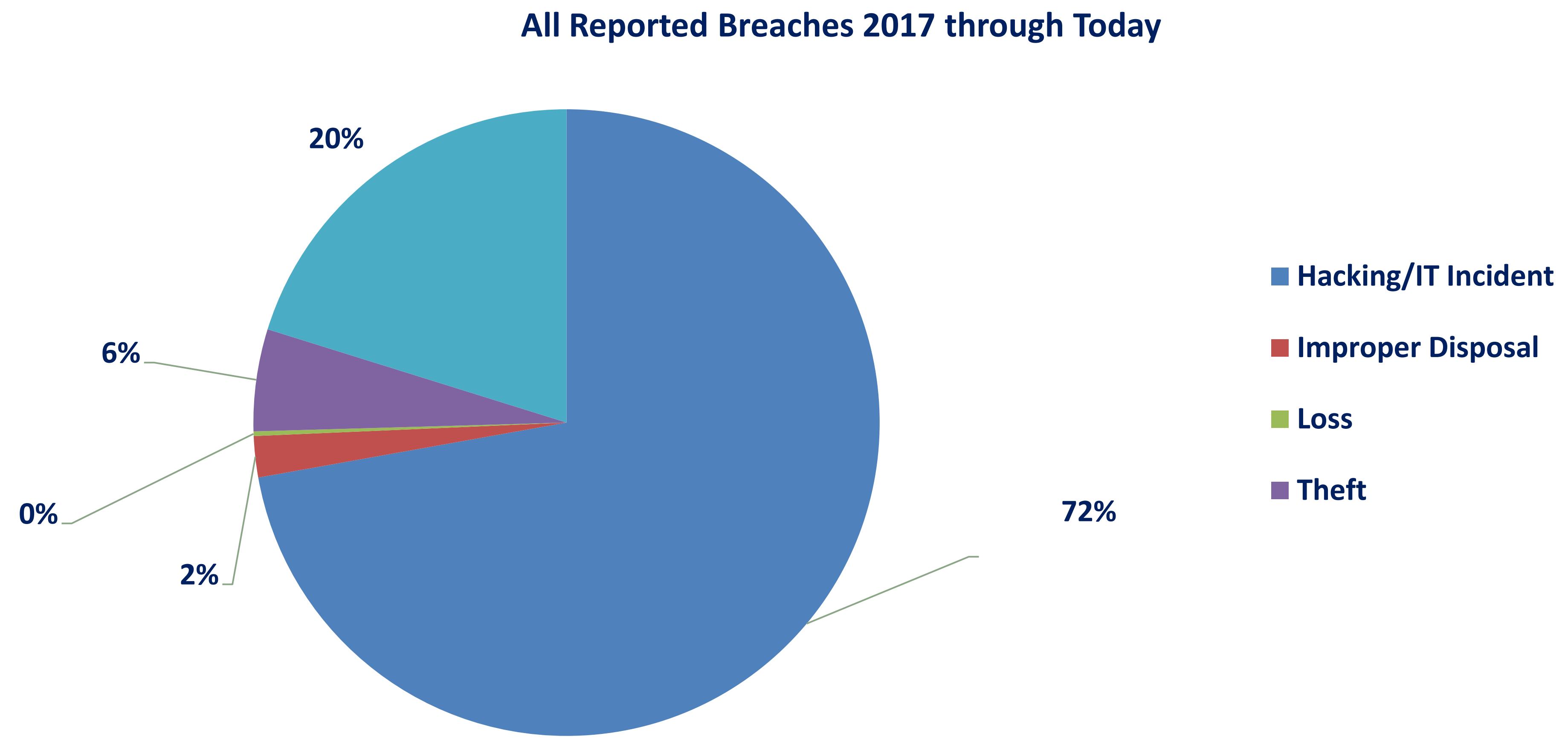
- You’re only as secure as your vendors.
- Ponemon, 2018 – 59% of organizations had data breaches caused by vendor vulnerabilities
- Recent examples

OCR Wall of Shame as of 8:42 am 4.24.2019

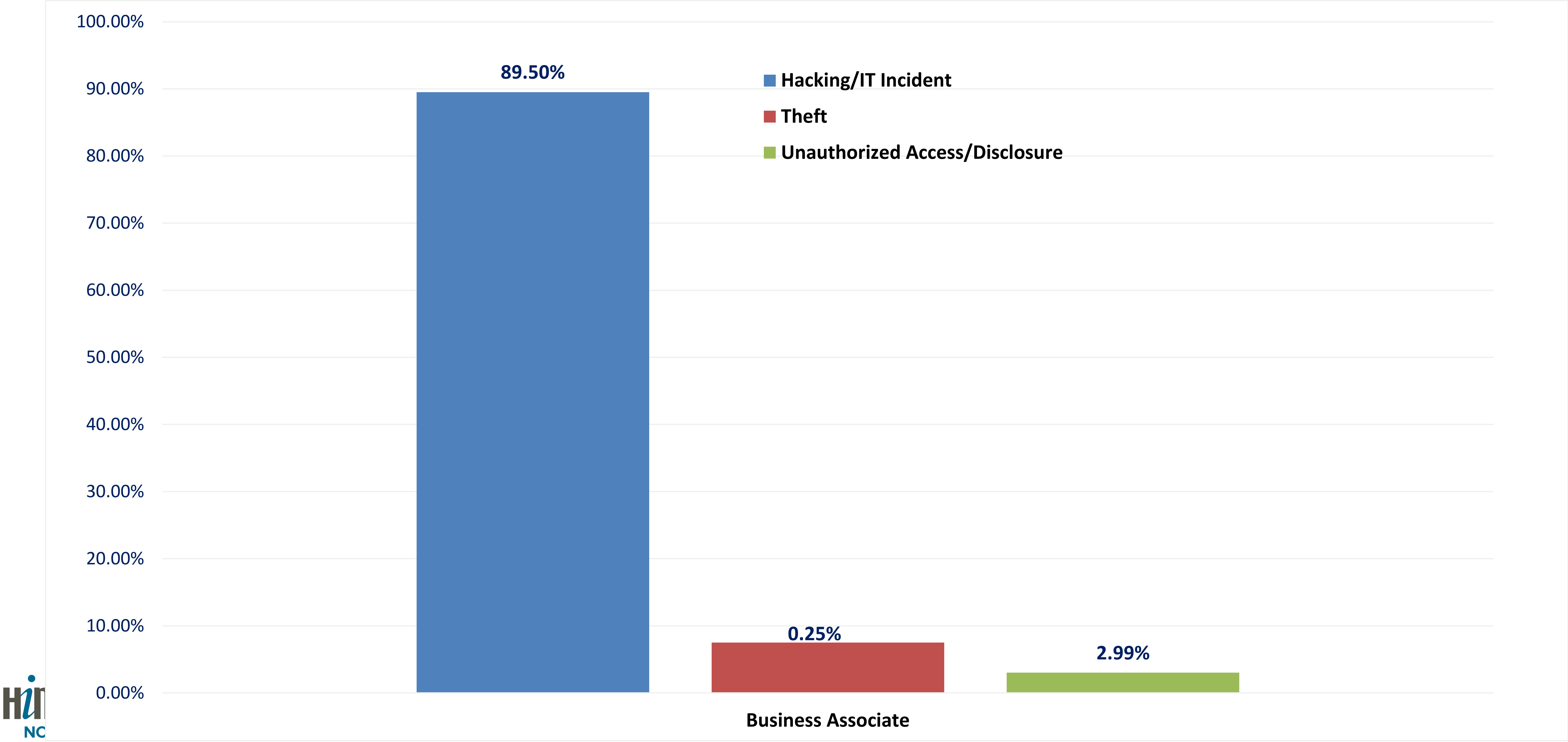


HIMSS NORTH CAROLINA Chapter

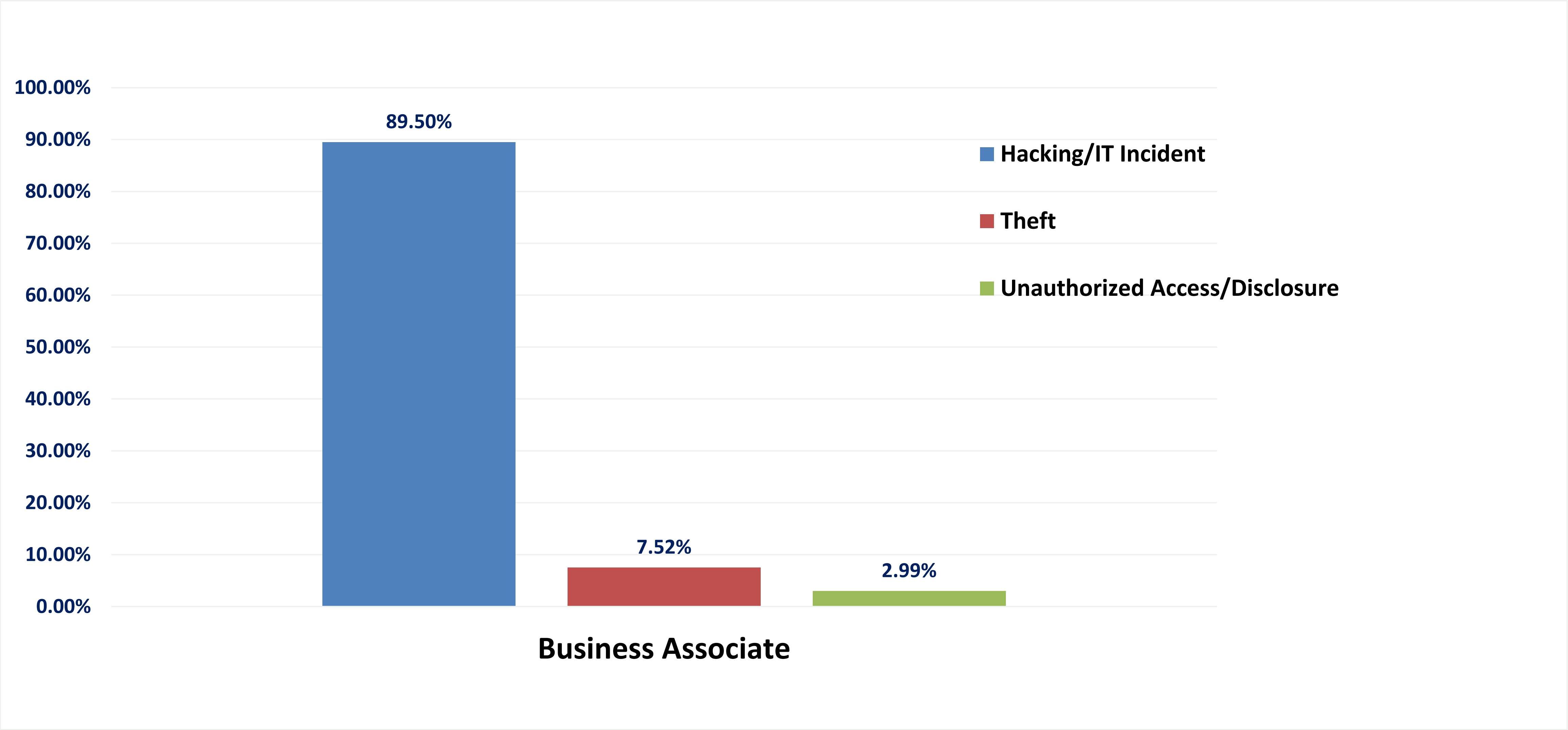
Types of Breaches



Business Associates – Type of Breach



Business Associates – 2019



HIMSS NORTH CAROLINA *Chapter*

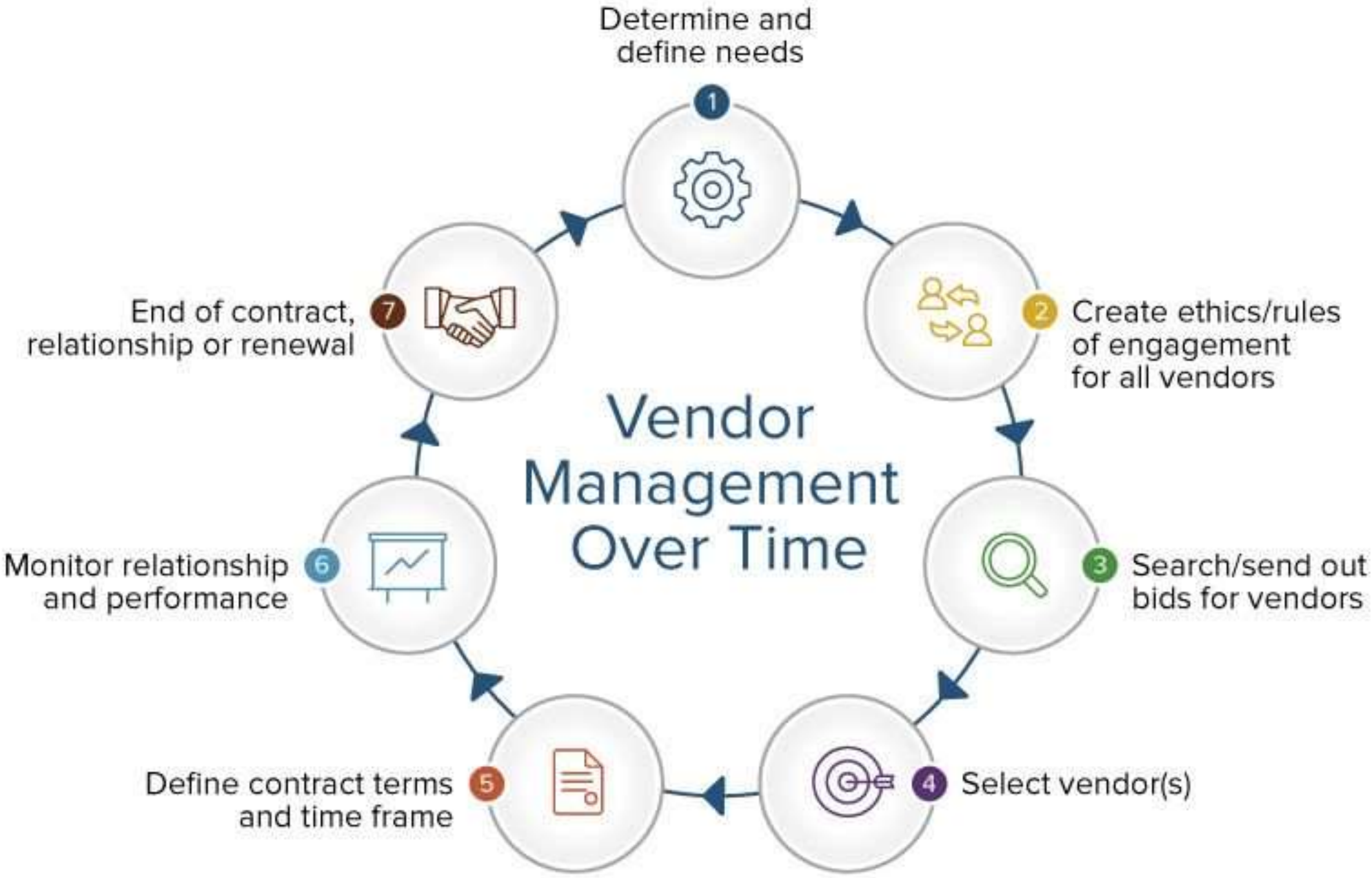
The Fundamentals

- Common approaches to VRM
- Federal and state regulations on privacy & security
- Increasingly complex environments
- Competitive market

Elements of a Vendor Risk Management Program

- Vendor inventory and classification
- Contract management
- Vendor risk assessments/due diligence questionnaires
- Ongoing supervision and monitoring of vendors

Managing your Vendors over Time


Determine and define needs
1
2
Create ethics/rules of engagement for all vendors
Vendor Management Over Time
3
Search/send out bids for vendors
4
Select vendor(s)
5
Define contract terms and time frame
6
Monitor relationship and performance
7
End of contract, relationship or renewal

HITRUST – The Basics

- The HITRUST Approach – a risk-based framework
  - ISO, NIST, PCI, HIPAA
- Applying the HITRUST Approach
  - Organizational risk factors reflect the value of the data shared with third parties
  - Compliance factors address fines or penalties an organization can face due to breach by a third party, which also influences the probable impact of a data compromise
  - Technical factors relate to how a third party accesses, processes, stores and/or disposes of an organization's data
- The Certification process
  - Covered Entity
  - Vendor
  - Assessor

All Together

- Vendor due diligence process
  - Initial questions
  - Continuous monitoring
- Consider replacing the questionnaire with the CSF Certification
  - Consistent methodology
  - Less time and effort for you and your team