

# THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING



# CYBERSECURITY—STEPS YOU CAN TAKE TO SECURE YOUR ORGANIZATION



April 27, 2017

# Introduction



**Keith Brooks**

Director

Peoria, IL

309.497.1467 Office

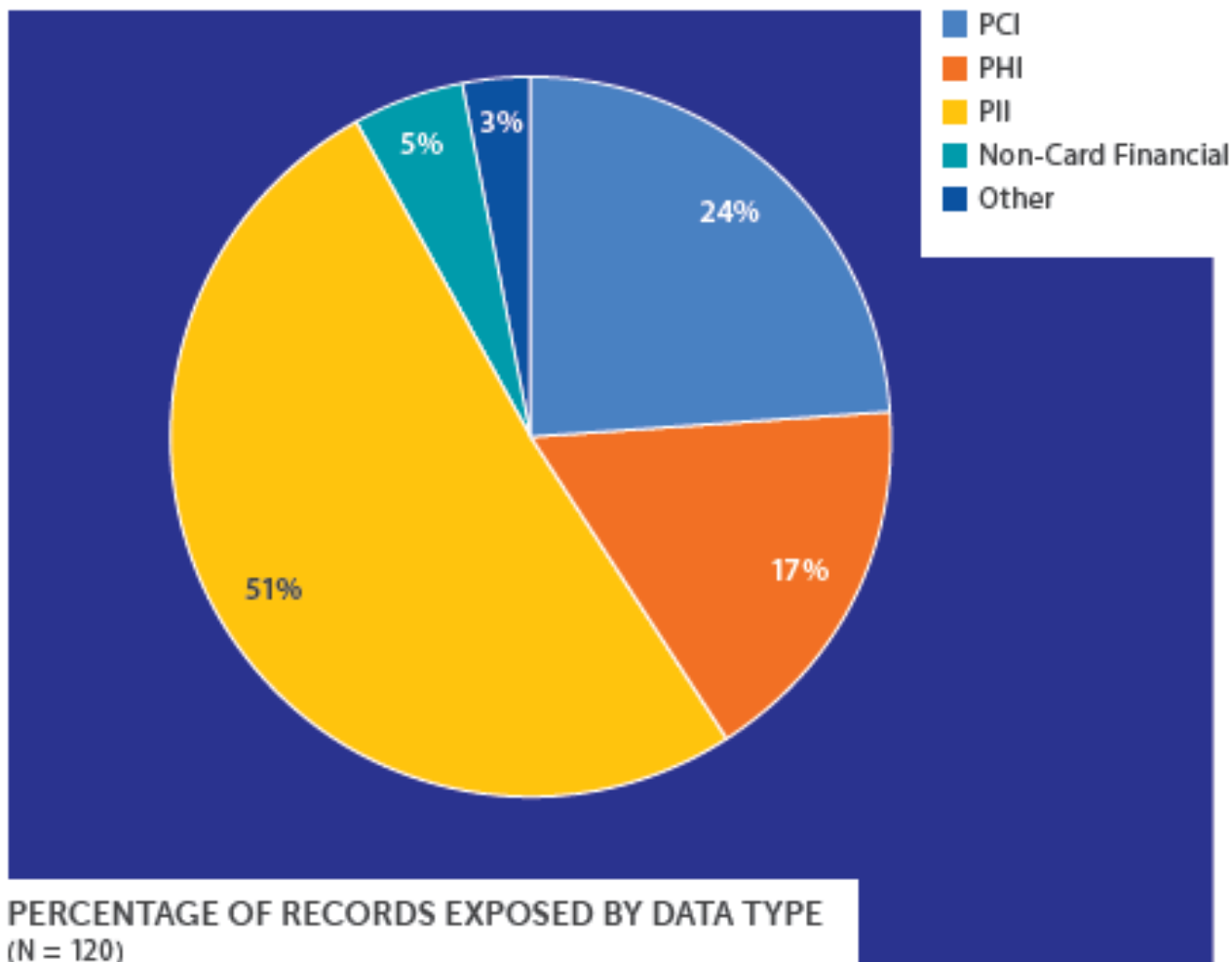
[keith.brooks@rsmus.com](mailto:keith.brooks@rsmus.com)

# CYBERSECURITY

The Latest Statistics

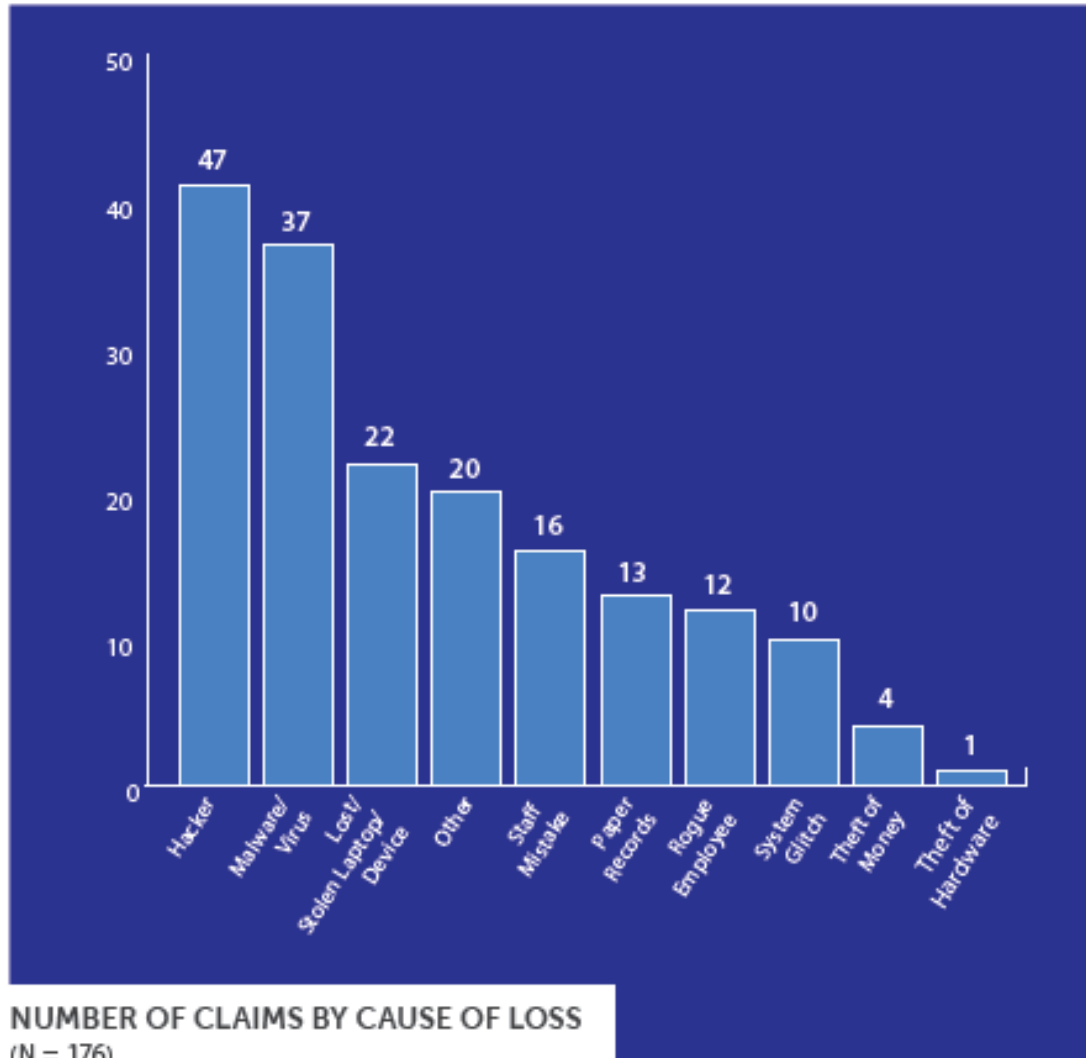
# Security Statistics

Compiled from:  
- NetDiligence/RSM 2016 Annual Cyber Claims Study



# Security Statistics (continued)

Compiled from:  
- NetDiligence/RSM 2016 Annual Cyber Claims Study



30% of breaches were due to insiders.

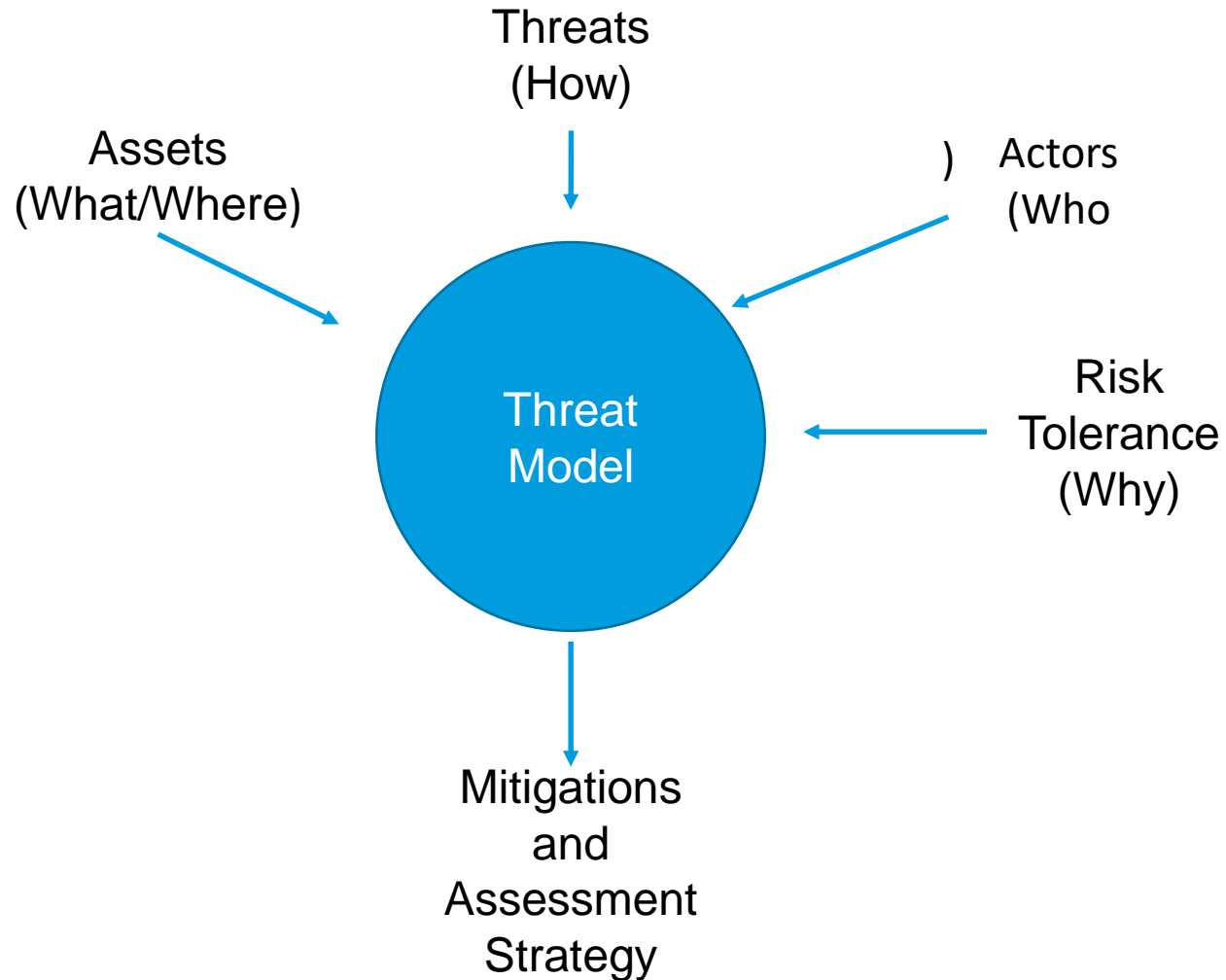
Of those, 77% were unintentional.

# CYBERSECURITY

## Threat Overview



# Threat Modeling Methodology



# Threat Modeling Methodology (*continued*)

(Actors) Who are the bad actors you're concerned with?

- Employee
- Contractor
- Customer
- Random attacker
- Focused attacker
- State-sponsored attacker

(Threats) How are the bad actors going to attack you?

- From the Internet
- From your internal network
- From your wireless network
- Via Email
- From USB keys
- From the phone

(Assets) What data do they want?

Customer records  
Employee records  
Money transfer  
Money laundering  
Ransomware

(Risk Tolerance) Every "scenario" has a cost. What is your risk tolerance?

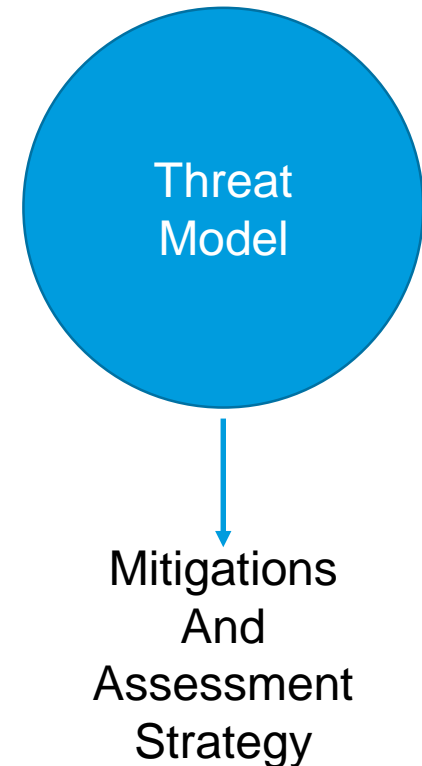
- Financial risk
- Brand risk
- Operational risk

# Mitigations

The result is a set of scenarios that are most important to you.

You use these scenarios to:

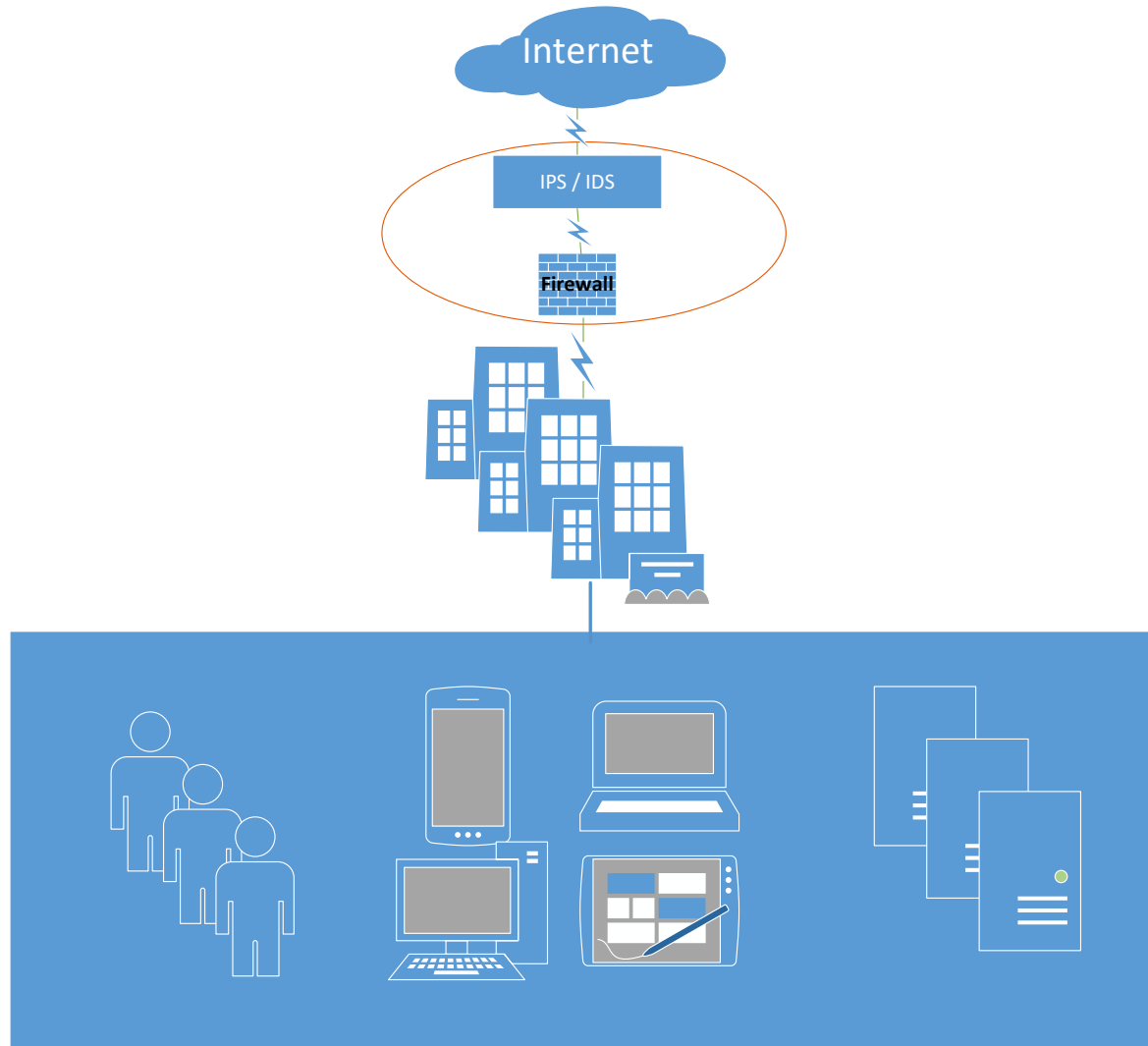
- Assess the likeliness of being impacted from them
- Build a strategy to protect yourself against them
- Hedge your losses against them with cyberinsurance
- Accept the risk



# WHAT STEPS CAN YOU TAKE TODAY TO CONTROL RISK?

Threat Overview

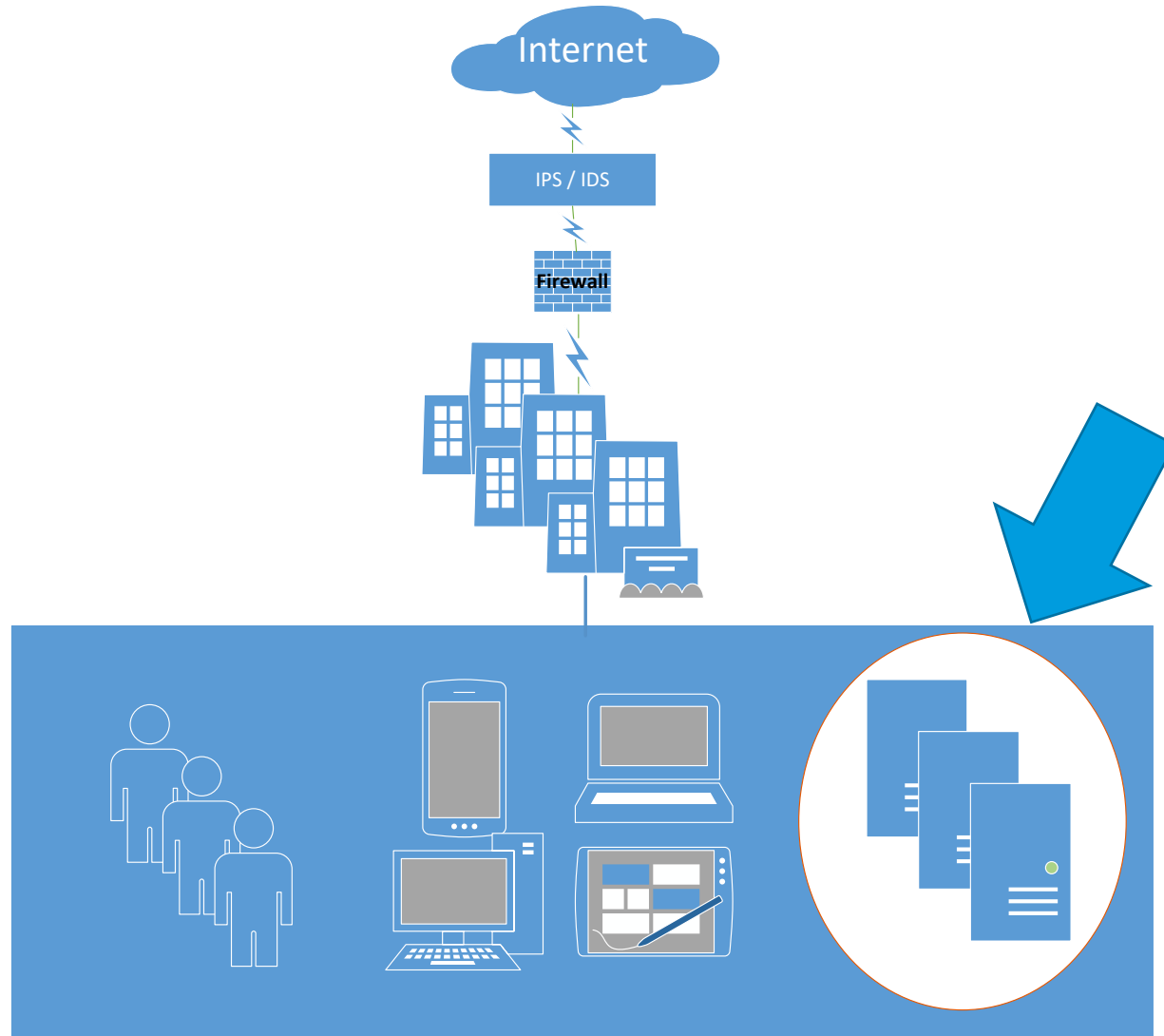
# Build Your Strategy



# Build Your Strategy *(continued)*

- Network Borders
  - Advanced Firewall Technology
    - Establish regular cadence for rule review and device updates to ensure optimal protection.
  - Intrusion Detection & Prevention Systems
    - Provides bi-directional coverage
    - Outsource to a dedicated provider or bring specialized staff in house to manage.
    - Regular review and update cadence is key to successful performance

# Build Your Strategy *(continued)*

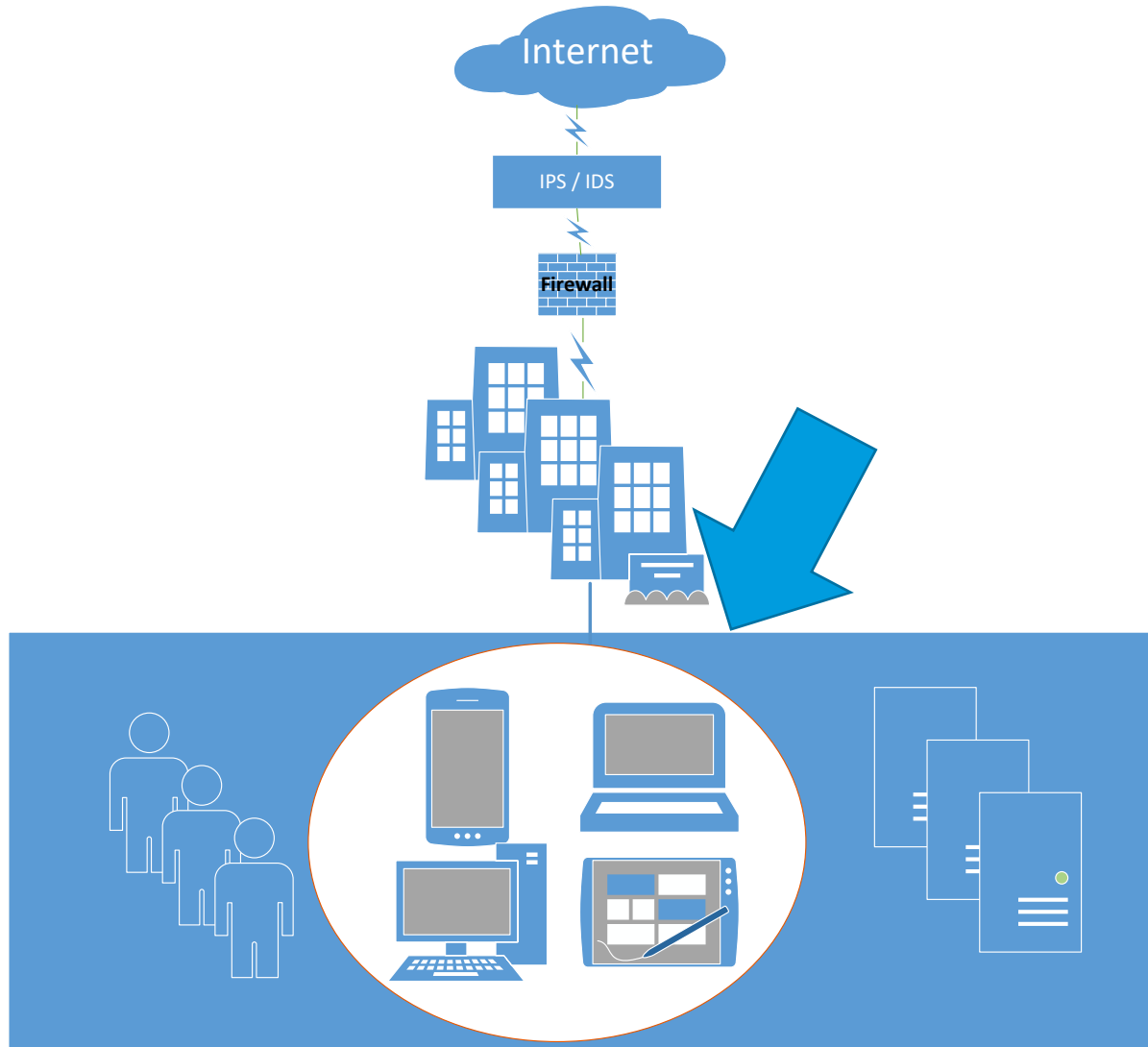


## Build Your Strategy *(continued)*

- Business Continuity & Disaster Recovery
  - Evaluate and test the organization's current BCP/DR posture
  - Test recovery of data and systems quarterly
  - Tabletop Test With Users
  - Evaluate fit of standing solutions against current market offerings:
    - Second site – Legacy DR, internally managed
    - Hybrid cloud – Heavy administration, co-managed
    - Cloud centric solutions – low administration, may be completely provider managed



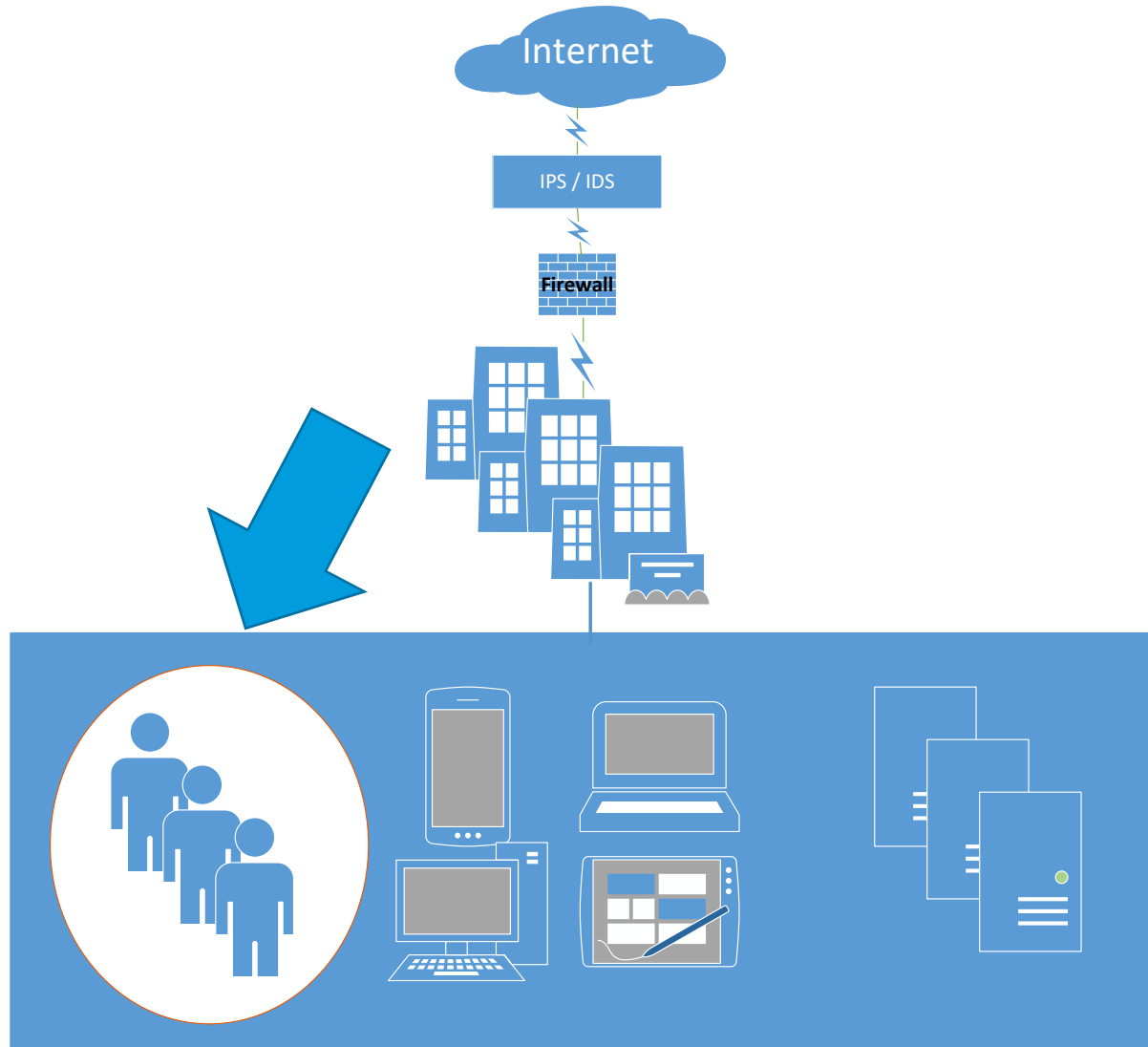
# Build Your Strategy (continued)



# Build Your Strategy *(continued)*

- Endpoints
  - Couple Antivirus Packages with Data Loss Prevention systems
    - Helps to control data proliferation and manage risk of data loss
  - Leverage Application Whitelisting Technology
    - Minimizes the threat posed by ransomware and other malicious software in the environment and on organizational systems
  - Encrypt All Data And Drives
    - Controls the risk of data theft on stolen systems
  - Centralized Management Of Each Is Key To Success!

# Build Your Strategy *(continued)*



# Build Your Strategy *(continued)*


- Related Policies To Protect The Organization
  - Acceptable Use Policy
    - Establishes guidelines around data and system usage with user community and provides enforceable guardrails for management
  - Cloud Use Policy
    - Provides baselines for acceptable use of cloud technologies
  - Data Handling Policies
    - Define data and information types that require special handling and attention

# Build Your Strategy *(continued)*

- Users
  - Educate users on risks
  - Ongoing education and risk testing of users
  - Retrain as needed based on testing outcomes
- Insurance
  - Cybersecurity, etc.
- Trust But Verify!
  - Establish recurring testing procedures
  - Regular assessment and audit cycles protect the organization



# QUESTIONS AND ANSWERS?



This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit [rsmus.com/about-us](http://rsmus.com/about-us) for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2017 RSM US LLP. All Rights Reserved.