The Federal Reserve Bank of Boston's

2017 Cybersecurity Conference

Federal Reserve
Bank of Boston™

The Benefits of Threat Sharing, a Case Study

Boston Fed Cyber Threat Sharing Genesis

Driving Factors

Implementation of a cohesive information security strategy continues to become both more costly and complex.

Increasing numbers of organizations are confronting strategic decisions on how best to secure their companies' most important assets.

Call to Action

At a 2013 meeting of the Federal Advisory Committee (FAC), members discussed the inability of US depository institutions (DIs) to effectively share cyber-threat information between one another.

Members noted: the Fed could expand its role by providing cyber security advisory services as a trusted interlocutor between banks and other government agencies.

Federal Reserve Capability

The FRBB has both local and national expertise in cyber security and threat sharing experience as a member of the Advanced Cyber Security Center (ACSC).

In addition to playing a role as a convener, there may be a role for the Fed in helping organizations with cyber security as well.

Our Program

Trusted Forum of Peers

- Similar Challenges
- Share Problems and Solutions
- Build Network

Threat Sharing

- Consolidated
- Targeted
- Actionable

Guest Speakers

- Emerging Trends
- Areas of Focus

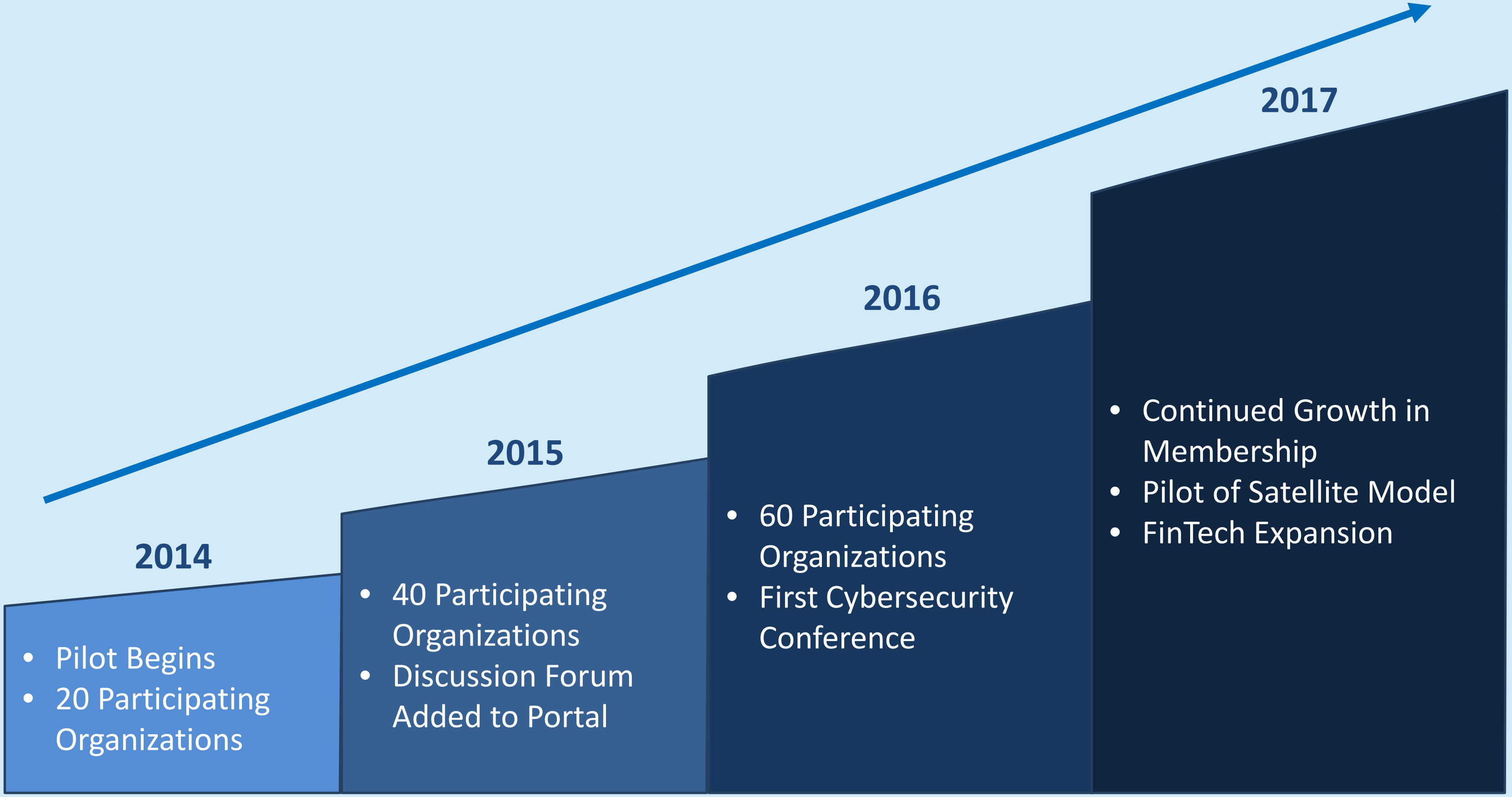
Best Practices

- Subject Matter Experts
- Topics of Interest

Member Roundtable

- Sounding Board
- Current Issues
- Creative Solutions

Growth and Evolution



2014

- Pilot Begins
- 20 Participating Organizations

2015

- 40 Participating Organizations
- Discussion Forum Added to Portal

2016

- 60 Participating Organizations
- First Cybersecurity Conference

2017

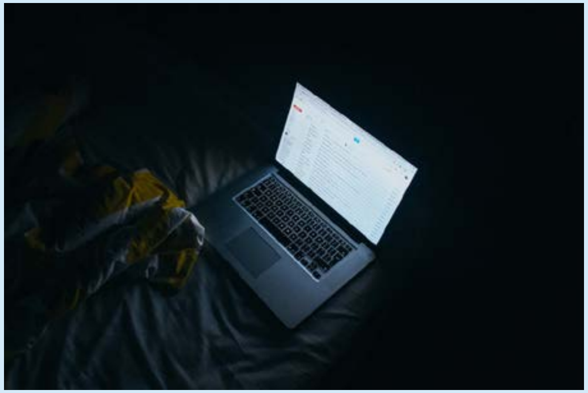
- Continued Growth in Membership
- Pilot of Satellite Model
- FinTech Expansion

Threat Sharing Grabs The Headlines …

- …But being able to discuss best practice is where the true value lies
- The first area discussed in our opening meeting led to widespread adoption or policy changes
- It was the first of many such changes in participating organizations

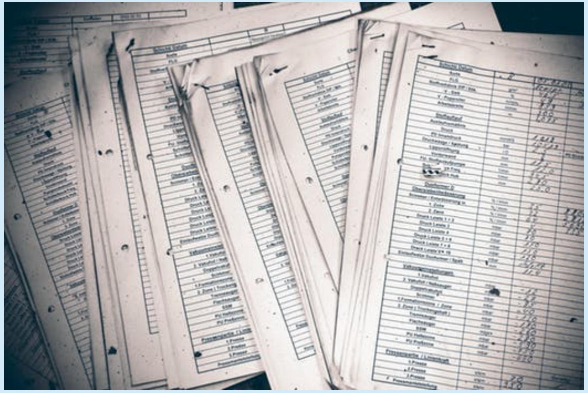
Sharing is Caring

Social Engineering Exercises



Mobile device management

Security Capabilities Inventory



External Email Flagging

The Information Economy

Making sure the board is adequately informed of cyber risks

ATM Skimmers in CT

What to do about domain name squatters

Ramifications of large data breaches

Approach to take when customer is using outdated Operating System or web browser

How to manage risks associated with cloud vendors

Ransomware

Whitelisting vs. blacklisting

ATM Malware

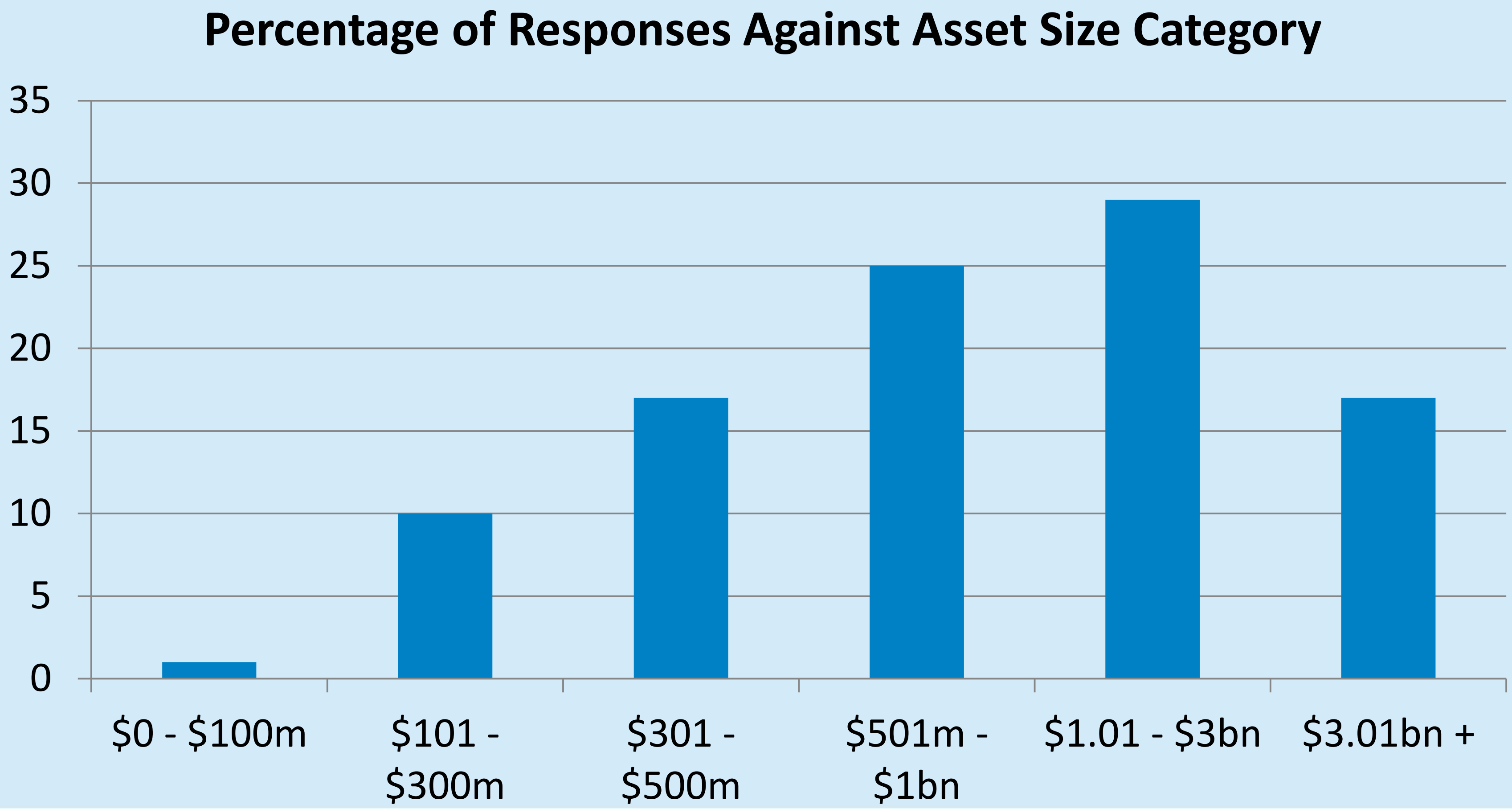
Incorporating the Internet of Things (IoT) into existing policy

Potential mitigation against DDoS attacks

Addressing vulnerabilities in products where support has ended

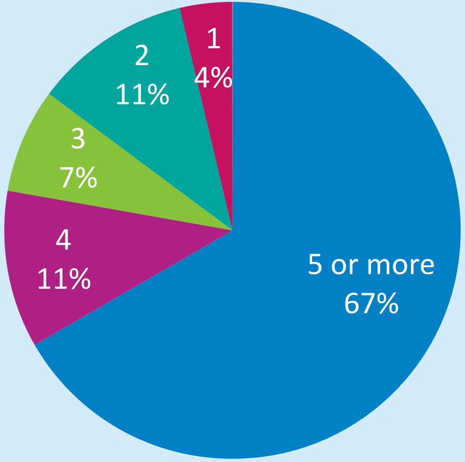
Email account compromise

Using Context to Justify Investment

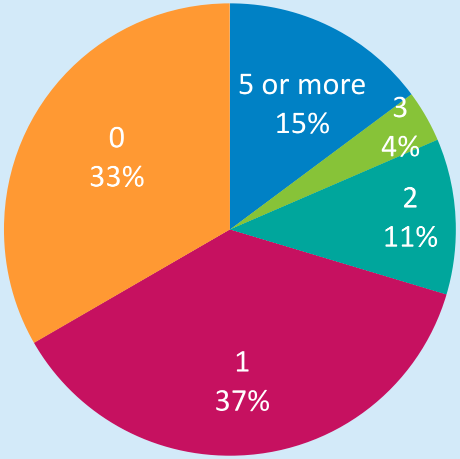


IT and InfoSec Bandwidth

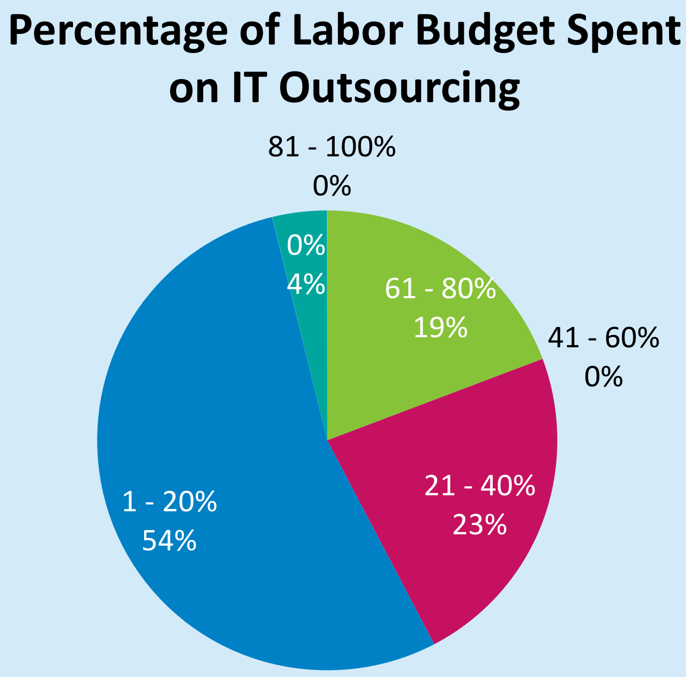
IT FTEs per Participating Organization

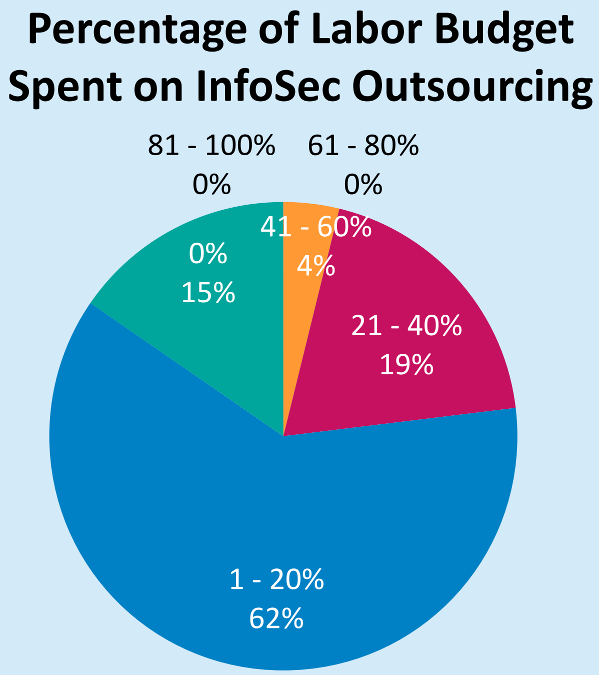


InfoSec FTEs per Participating Organization



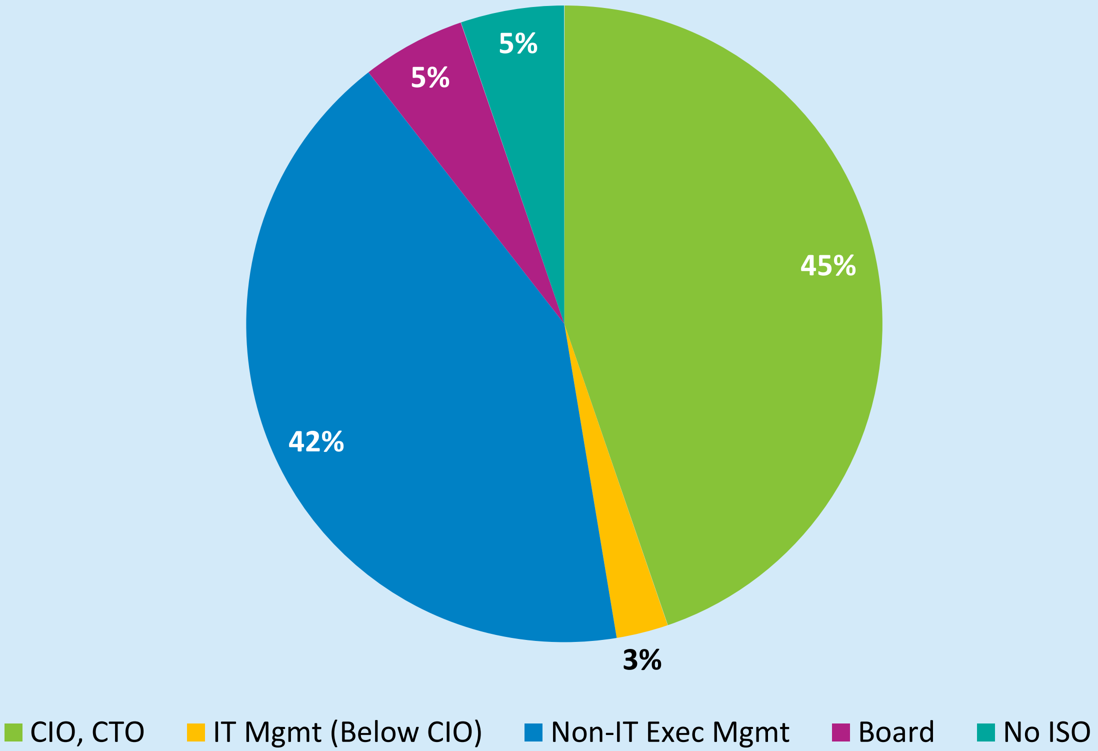
IT Outsourcing


Percentage of Labor Budget Spent on IT Outsourcing


Percentage of Labor Budget Spent on InfoSec Outsourcing

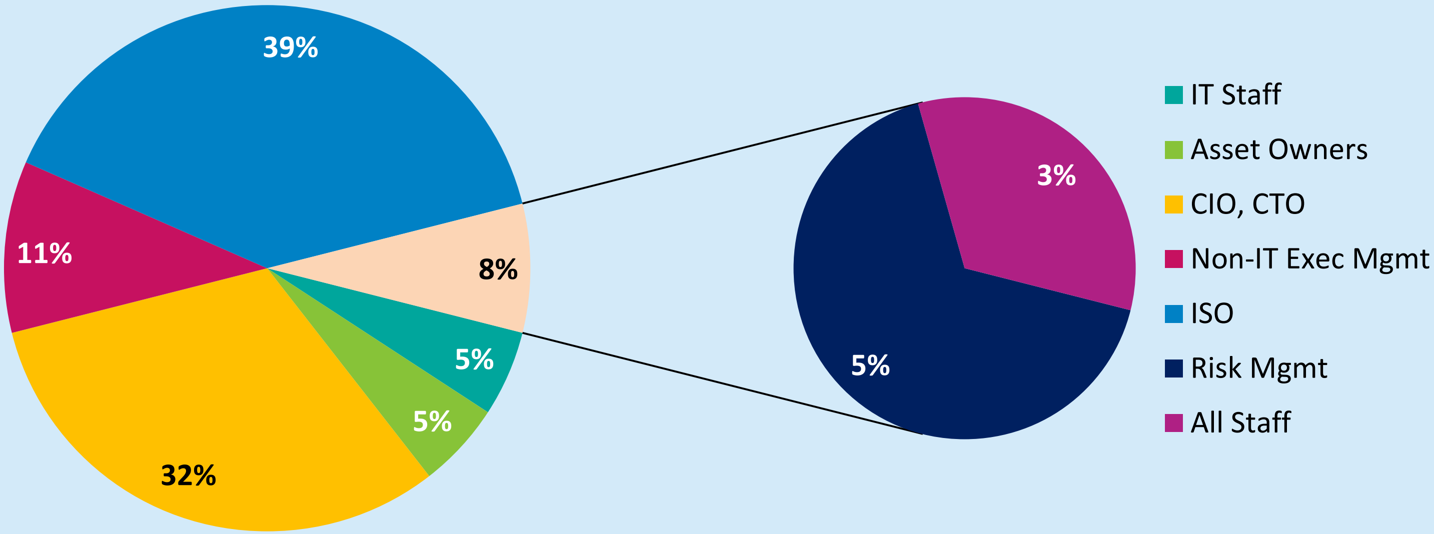
IT Governance

Reporting Structure for Information Security Leadership

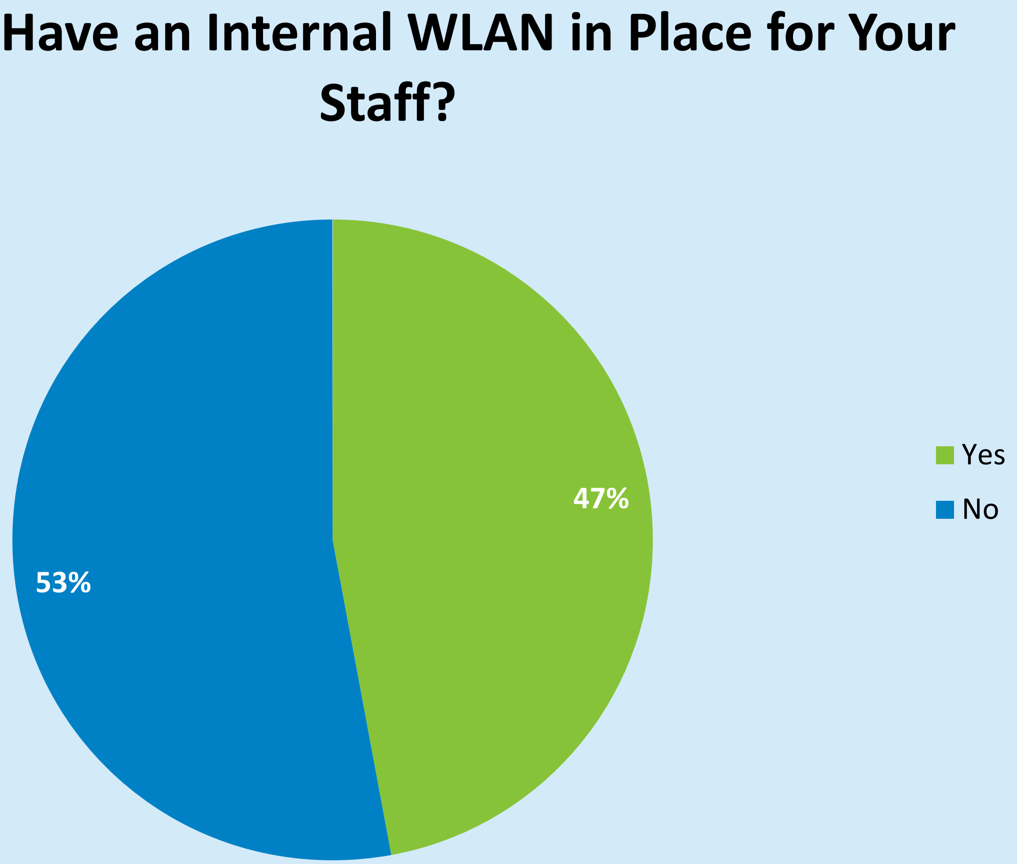


IT Governance

Accountability for Information Security Risks

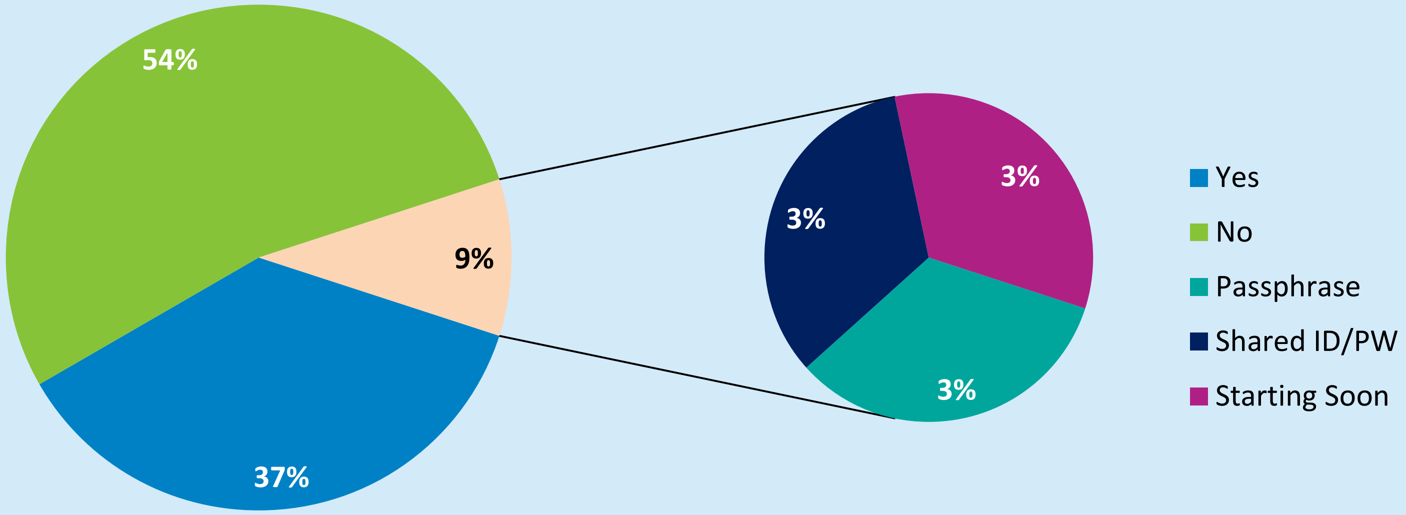


Wireless Access

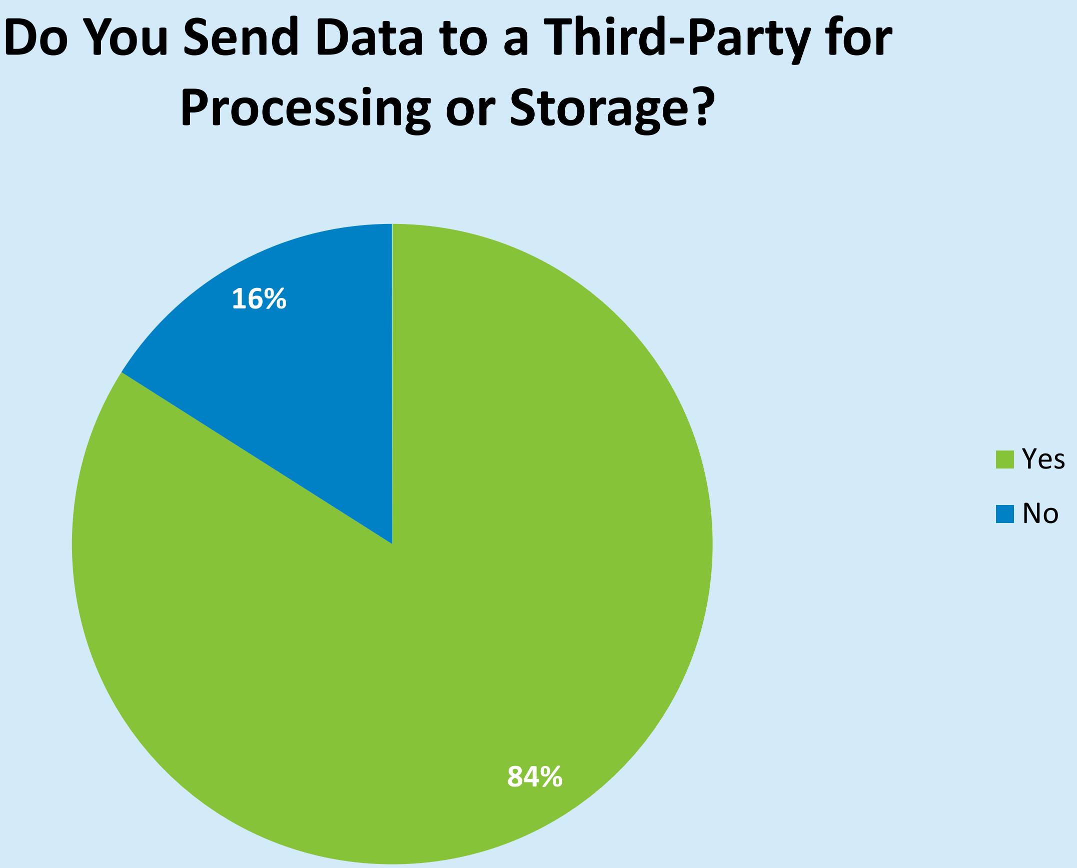


Wireless Access

Are Users of Your Guest Wireless Network Required to Enter a Unique ID & Password?



Use of Third Parties



Emerging Trends and Concerns

Identity and Access Management

Insider Risk

Fedwire Security

Blockchain

Cybersecurity Legal Considerations

Network Access Control

Threat Hunting