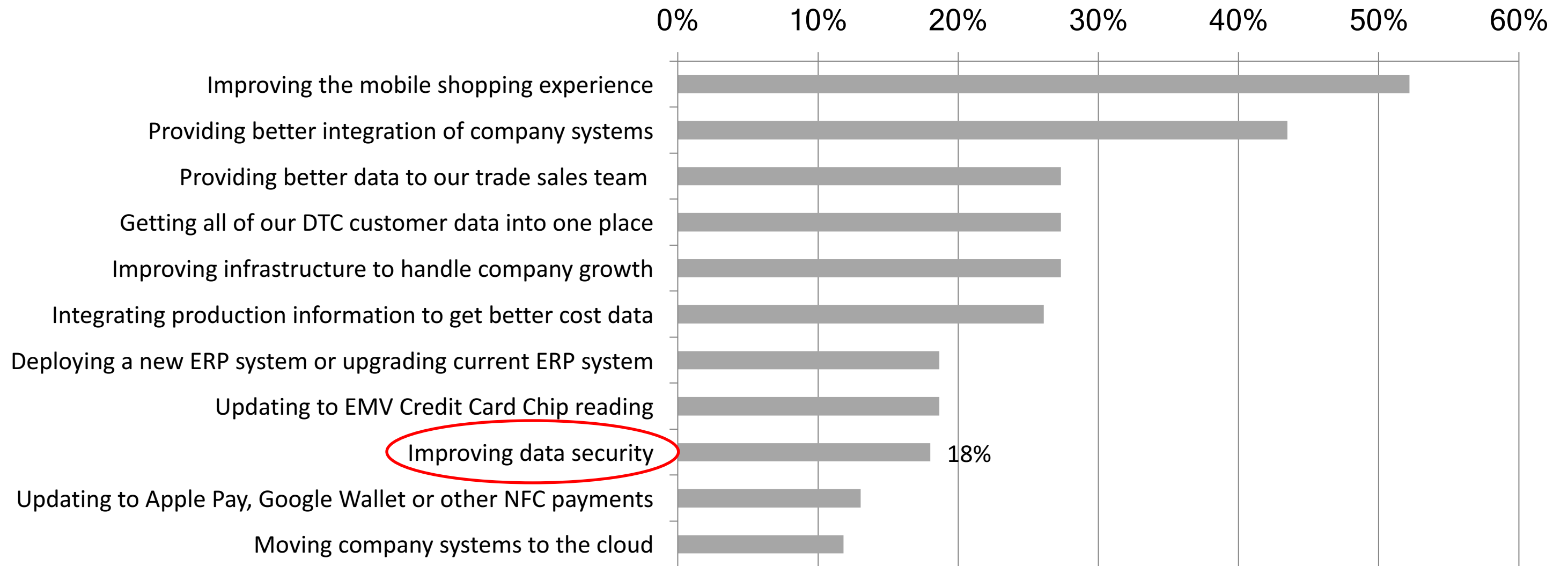


WINE INDUSTRY

**TECHNOLOGY**

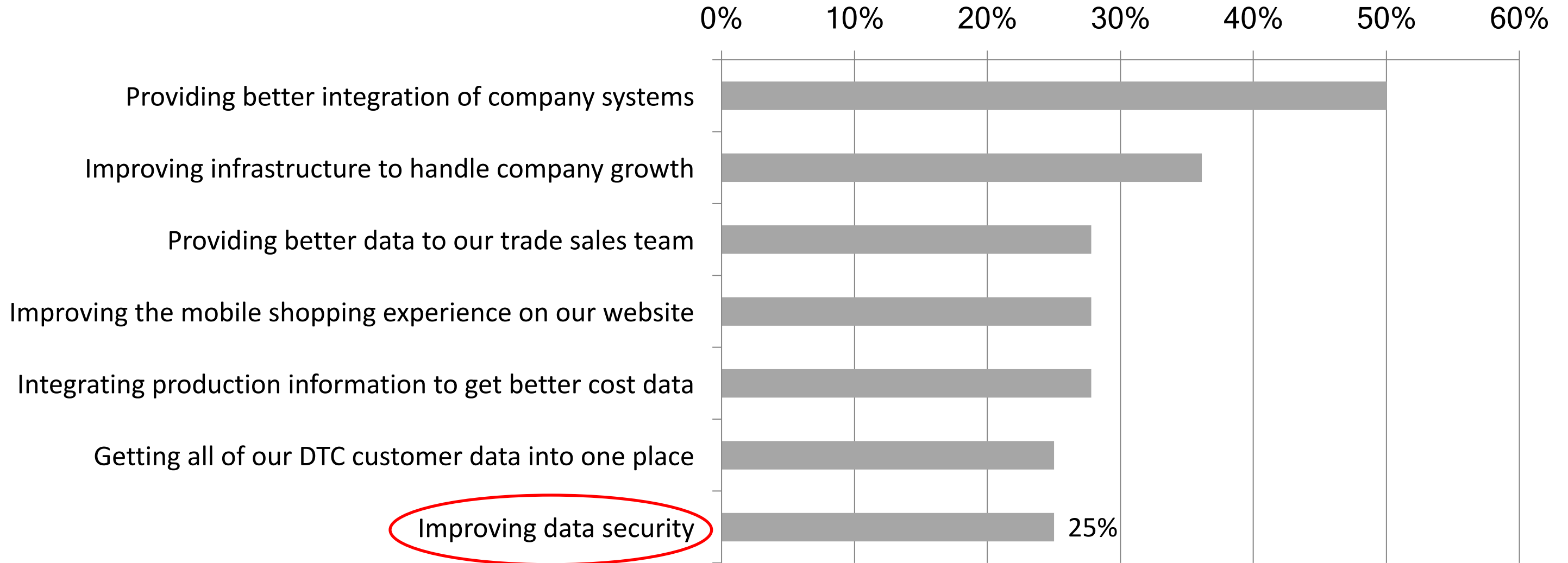
SYMPOSIUM

# What are the top 3 IT issues your company is looking to solve?



# What are the top 3 IT issues your company is looking to solve?

## - IT Managers



# Defending Your Company Against Cyber Attacks

- Charlie Lindell
  - IT Manager, Kistler Vineyards
- Glen Sorensen
  - IT Security Engineer, Ste. Michelle Wine Estates

# Agenda

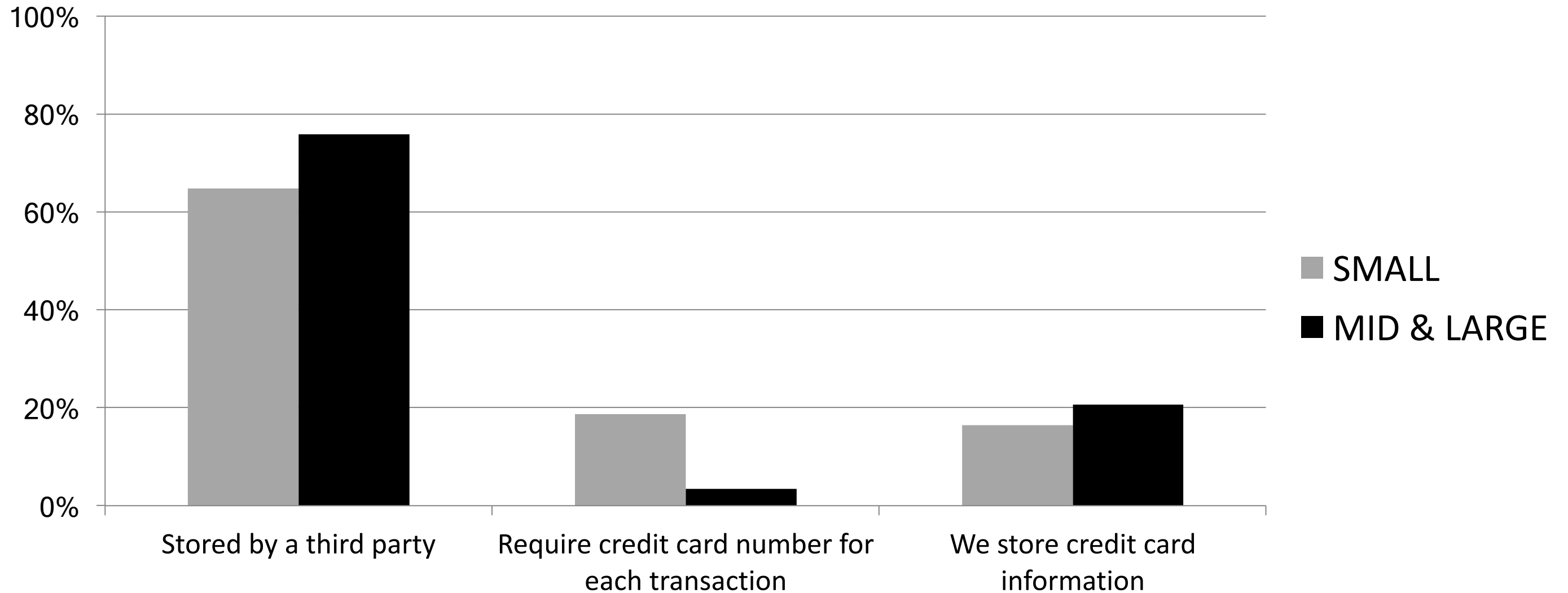
- Assessment
- Credit Cards
- The Cloud
- Takeaways
- Questions

# Assessment

- Asset Inventory
  - Mobile phones
- What devices are accessing your network
  - Separate network for guests
- Vendors
- What cloud services are being used

# Credit Card Security

For direct-to-consumer transactions, which best describes your winery?



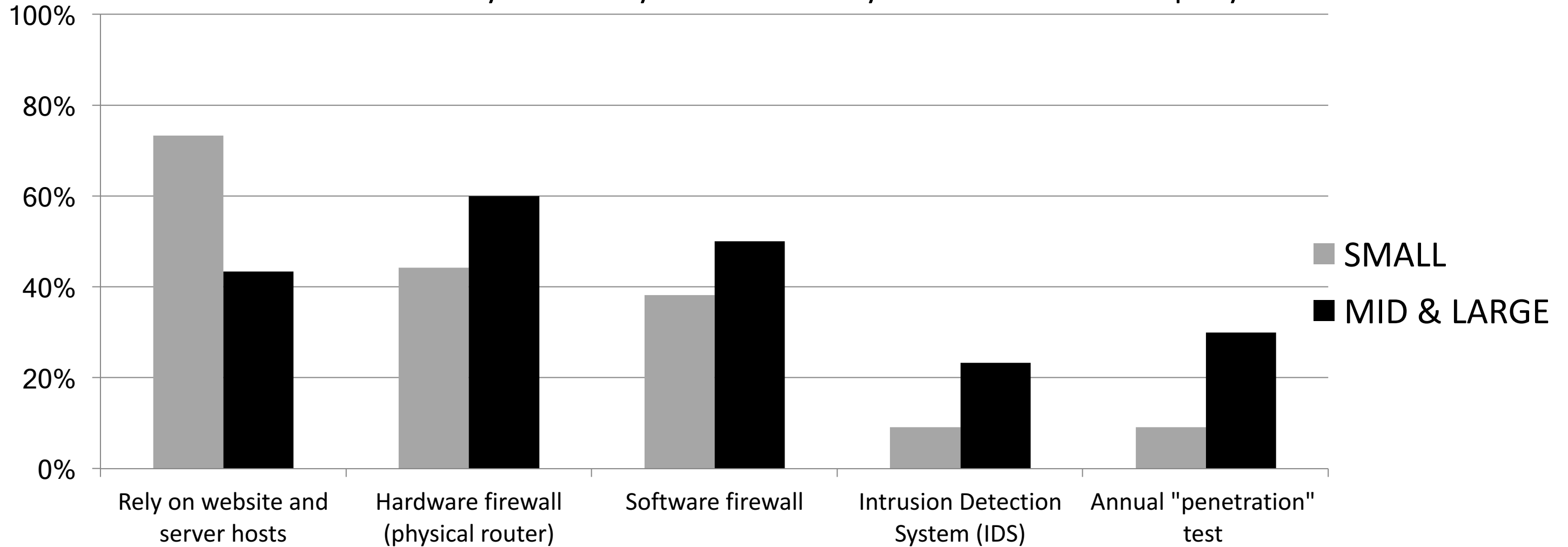
# Credit Card Compliance

- Storing credit cards on your servers vs. third-party
- Tokens
- The future of credit card handling

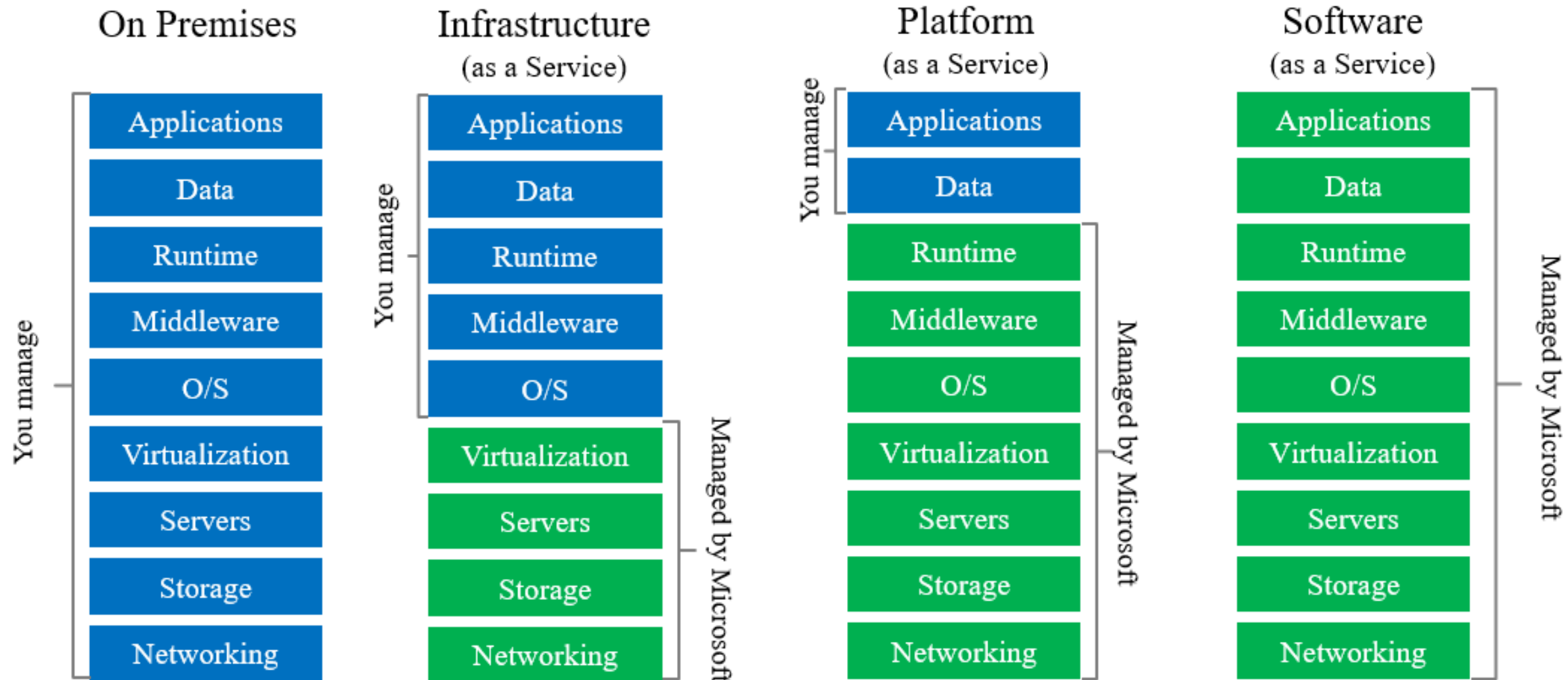


# Securing Your Company's Servers

What measures does your winery take to secure your website and company servers?



# Cloud Shared Responsibility



<https://thuansoldier.net/5200/>

# Takeaways

- Training
- Focus on security basics
- Quickly detecting and responding

# Training

- Security principles for management
  - Getting management on board
- Technical security for IT professionals
- Security awareness training for everyone
  - Training employees not to click

# Places to get Security Training

- SANS Institute - [sans.org](https://sans.org)
- Cybersecurity Academy – [cybersecurityacademy.com](https://cybersecurityacademy.com)
- Cybrary.it – free online training

# Focus On Security Basics

- Keep on patching...
  - Keep your systems updated and patched
- Email controls
- Passwords
  - Require complex passwords of 12 characters or more with three different character types
- Disable devices not being used

# Detecting and Responding

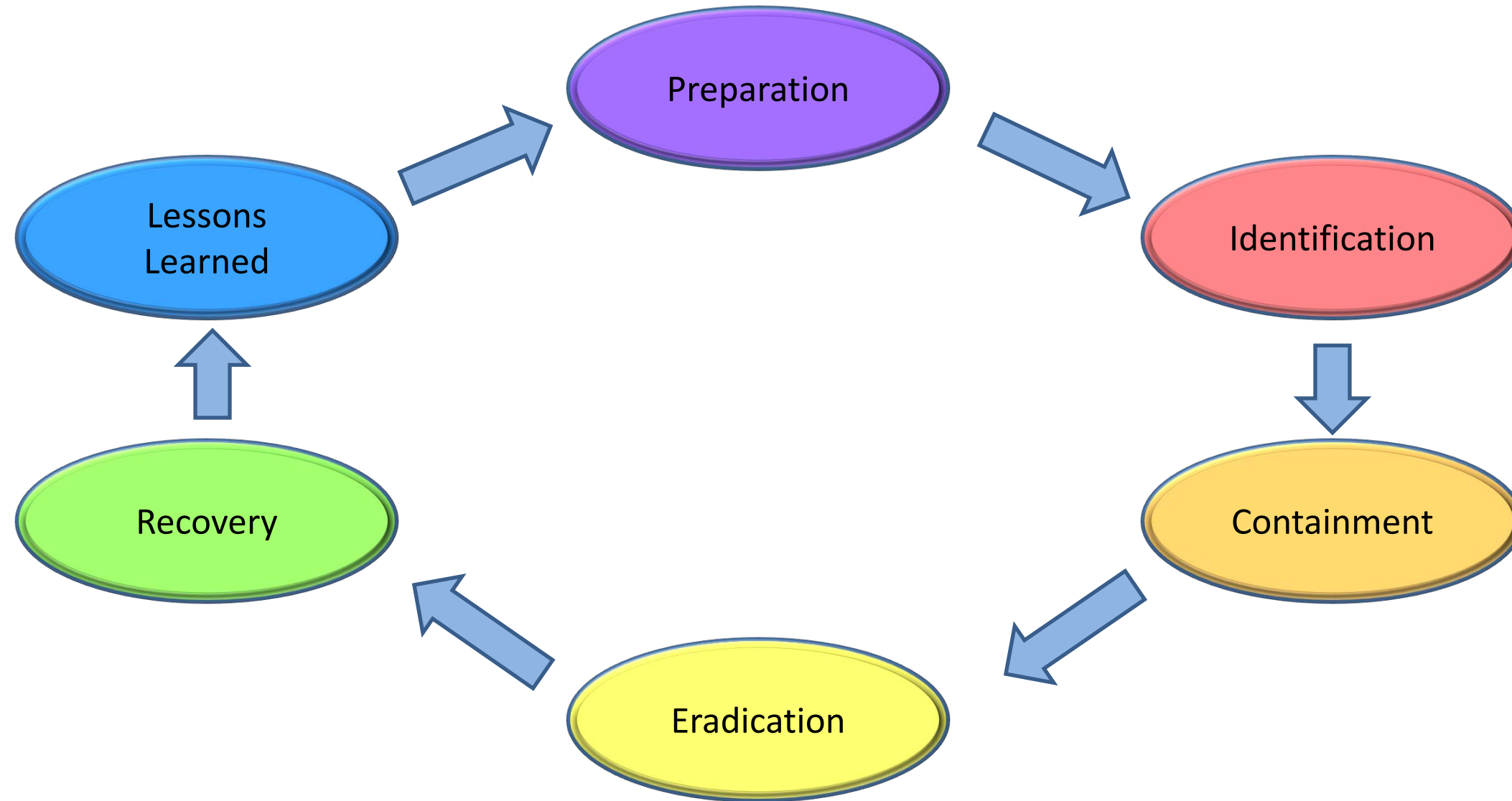
- Asset inventory
- Security monitoring
  - Use a Unified Threat Management (UTM) system to protect your assets

# Detecting and Responding

- Threat intelligence
  - US-CERT – [www.us-cert.gov](http://www.us-cert.gov)
  - SANS Internet Storm Center – [isc.sans.edu](http://isc.sans.edu)
  - CI Security Daily Blast – [ci.security/news/daily-news](http://ci.security/news/daily-news)
  - Social Media



# Incident Response



# Incident Response

- 1) **Preparation** - Incident response team, current contacts lists, tools
- 2) **Identification** - Document the situation, actions, and artifacts
- 3) **Containment** - Patching, isolation from the network/internet
- 4) **Eradication** - Removing malware, re-imaging
- 5) **Recovery** - Restoring business function, monitoring
- 6) **Lessons Learned** - How can we ensure similar doesn't happen again?

# Questions