WINE INDUSTRY
TECHNOLOGY
SYMPOSIUM
What are the top 3 IT issues your company is looking to solve?

- Improving the mobile shopping experience
- Providing better integration of company systems
- Providing better data to our trade sales team
- Getting all of our DTC customer data into one place
- Improving infrastructure to handle company growth
- Integrating production information to get better cost data
- Deploying a new ERP system or upgrading current ERP system
- Updating to EMV Credit Card Chip reading
- Improving data security
- Updating to Apple Pay, Google Wallet or other NFC payments
- Moving company systems to the cloud

Improving data security: 18%
What are the top 3 IT issues your company is looking to solve?

- IT Managers

0% 10% 20% 30% 40% 50% 60%

- Providing better integration of company systems
- Improving infrastructure to handle company growth
- Providing better data to our trade sales team
- Improving the mobile shopping experience on our website
- Integrating production information to get better cost data
- Getting all of our DTC customer data into one place

Improving data security - 25%
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?

- Stored by a third party
- Require credit card number for each transaction
- We store credit card information

Bar chart showing percentages for each option:

- Stored by a third party: 80% (MID & LARGE), 60% (SMALL)
- Require credit card number for each transaction: 20% (MID & LARGE)
- We store credit card information: 40% (MID & LARGE), 20% (SMALL)
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?

- Rely on website and server hosts
- Hardware firewall (physical router)
- Software firewall
- Intrusion Detection System (IDS)
- Annual "penetration" test

Bar chart showing the percentage of wineries using various security measures, categorized by winery size (SMALL, MID & LARGE).
Cloud Shared Responsibility

On Premises
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

You manage

Infrastructure (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

You manage

Platform (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Managed by Microsoft

Software (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Managed by Microsoft

https://thuansoldier.net/5200/

August 21, 2018
Napa Valley Marriott
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
- Cybersecurity Academy – 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
  - SANS Internet Storm Center – isc.sans.edu
  - Social Media
Incident Response

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Flow: Preparation → Identification → Containment → Eradication → Recovery → Lessons Learned → Preparation
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