GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

National Restaurant Association

"Cybersecurity Framework for the Restaurant Industry"

"Cybersecurity 201, the Next Step"

Restaurant.org

National Restaurant Association

October 2017

URL:
https://www.restaurant.org/Downloads/PDFs/advocacy/cybersecurity201.pdf

Accessed: 02 July 2019

Synopsis: Governance (ID.GV)
The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
ID.GV-1: Organizational information security policy is established
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4: Governance and risk management processes address cybersecurity risks

NIST CATEGORY: Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

ID.GV-1 Organizational information security policy is established

How to apply in your restaurant:

1) Determine the regulatory and legal requirements for the restaurant's security and include this information in your security policies.
2) Update your security policies on a periodic basis.
3) An appropriate level of leadership (i.e., CIO, GC, CEO, etc.) should review and approve all information security policies.
4) Communicate the policy to all appropriate company employees (annually is recommended).
5) Maintain information security policies in a repository accessible by employees.

Anticipated outcomes if action completed:

Establishing an information security policy will educate employees on regulatory requirements and the importance of security. Your policies should include employee roles and responsibilities and expectations of conduct. Information security policies should be communicated throughout the organization.

CRITICALITY ●●●○○

DIFFICULTY ●●○

ID.GV-2 Information security roles & responsibilities are coordinated and aligned with internal roles and external partners

How to apply in your restaurant:

1) The IT subject matter expert in partnership with HR and functional areas (i.e., finance, legal, supply chain, operations) should establish the roles and responsibilities of employees and external partners for the use and access of company information systems.
2) IT should map internal roles and external partners to information systems. Ensure that the appropriate roles are aligned with the required information systems and equipment.
3) Job descriptions should note the information system(s) required to complete job duties. External partner agreements, contracts, statements of work or other documents should include the information systems required to complete business activities.

Anticipated outcomes if action completed:

Clearly document, communicate and align security roles and responsibilities within the organization and between the organization and any third-party providers. Maintain appropriate levels of access to systems or databases based on roles.

CRITICALITY ●●●○○

DIFFICULTY ●●○

ID.GV-3 Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

How to apply in your restaurant:

1) IT subject matter experts should be well informed of ever-changing industry standards and regulatory requirements, and provide ongoing updates to the organization.
2) IT subject matter experts should meet at least annually to discuss regulations and potential risks to the organization (see ID.RM-1).
3) Management should review requirements and risks to determine organizational risk tolerance and if additional controls are needed.

Anticipated outcomes if action completed:

The organization should be mindful of the constantly changing legal environment and industry standards related to cybersecurity. Subject matter experts must communicate and inform the organization of changes that impact the business and allow management to assess risk tolerance and determine if additional controls should be implemented.

CRITICALITY ●●●●●

DIFFICULTY ●●○

Governance (ID.GV) continued

ID.GV-4 Governance and risk management processes address cybersecurity risks

How to apply in your restaurant:

1) Meet with your board and/or management team at least annually to discuss risks to the company, including cybersecurity risks.
2) The discussion should include all potential cybersecurity risks, risk response plans and risk tolerance. Document the discussion and responses for review during the next meeting.
3) Ensure that your board and management are aligned on the risk level of cybersecurity in the organization, risk responses and risk tolerance.

Anticipated outcomes if action completed:

Cybersecurity risk management should be a part of the organization's regular risk-management processes and should include at least an annual executive level review of risk tolerance and risk response plans.

CRITICALITY

DIFFICULTY