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: Asset Management (ID.AM)
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

ID.AM-5
Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

ID.AM-6
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Asset Management (ID.AM) continued

ID.AM-5 Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value

How to apply in your restaurant:

1) Create a scoring system to identify the most critical to least critical technology systems.
2) List information systems from the most confidential and sensitive data to the least.
3) Determine the business value for each system.

Anticipated outcomes if action completed:

Prioritize your technology resources based on type of system, importance in achieving the business objective and value provided to the business. The priority can provide guidance to securing and upgrading your technology.

CRITICALITY

DIFFICULTY

ID.AM-6 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

How to apply in your restaurant:

1) Develop roles and responsibilities for your employees and third parties regarding information systems and cybersecurity. All information systems and equipment should be included.
2) Your procedures may include a definition of information systems (i.e., networks, software and the data they produce) and equipment (cell phone, laptops, etc.), ownership (i.e., owned by the company), descriptions of overall expectations and proper use (business and/or limited personal use), inappropriate/misuse (violations of policies or laws) and disciplinary actions.
3) The procedures should be documented and retained in a location accessible to all employees or physically distributed (via intranet, break rooms, employee handbook, orientation packet, code of conduct, etc.). For third parties, the content should be included in appropriate supplier/vendor codes of conduct or in contractual agreements.

Anticipated outcomes if action completed:

Establish, document and communicate the cybersecurity roles and responsibilities of employees and third parties. These activities allow the organization to communicate expectations and proper use of information systems and assets.

CRITICALITY

DIFFICULTY