Restaurant Technology Network

join. share. thrive.

Restaurant Cybersecurity Operations

Guidance to help restaurants predict, prevent, detect and respond to cybersecurity attacks, as well as how to structure overall security operations.

Introduction

Quick-serve and fast casual restaurants are a perennial top target for cyber attacks due to the decentralized nature and high volume of credit card transactions, and thus have unique cybersecurity requirements. Cybersecurity is not a "set it and forget it" endeavor; a successful operation must include both the right technology and the right staff level and expertise to drive it. The speed at which restaurants operate plays a vital role in restaurant cybersecurity operations, which must take into consideration IT network performance, ease of management, and rapid store deployment. Complicating restaurant cybersecurity even further is the mandate to rally franchisees and corporate stores around a standardized security operation, which can prove to be a difficult change management project. As such, developing a powerful yet practical cybersecurity operation, inclusive of third parties, is critical for every size of organization.

This RTN technical guidance document provides best practice intelligence around how to predict, prevent, detect and respond to cybersecurity attacks, and includes some guidance around Defense-in-Depth and Threat Lifecycle, which can help restaurants develop a comprehensive set of controls for security operations.

Staff

ABBY LORDEN
VP and Brand Director, *HT*
Co-Founder, RTN
973.607.1358
alorden@ensembleiq.com

ANGELA DIFFLY
Co-Founder, RTN
404.550.7789
angela@restauranttechnologynetwork.com

PATRICK DUNPHY
CIO, HTNG & RTN
312.690.5039
patrick@restauranttechnologynetwork.com

ROBERT FIRPO-CAPPIELLO
Editor in Chief, *HT*
917.208.7393
rfirpo-cappiello@ensembleiq.com

ANNA WOLFE
Senior Editor, *HT*
207.773.1154
awolfe@ensembleiq.com

KATHERINE WARE
Senior Account Executive, *HT* & RTN
785.424.7392
kware@ensembleiq.com

NOELL DIMMIG
Account Executive, *HT* & RTN
973.607.1370
ndimmig@ensembleiq.com

MOLLY MCLOONE
Brand Marketing Manager, *HT* & RTN
908.433.2796
mmcloone@ensembleiq.com

TAMMY HANSON
Membership Manager, RTN
314.570.4798
tammy@restauranttechnologynetwork.com

Table of Contents

RTN Mission

The Restaurant Technology Network (RTN) is a membership community solely dedicated to the restaurant technology industry. Through access to valuable benefits and powerful connections, our members shape industry standards and share technical guidance to help restaurateurs run successful businesses and better serve their customers.

Key Contributors

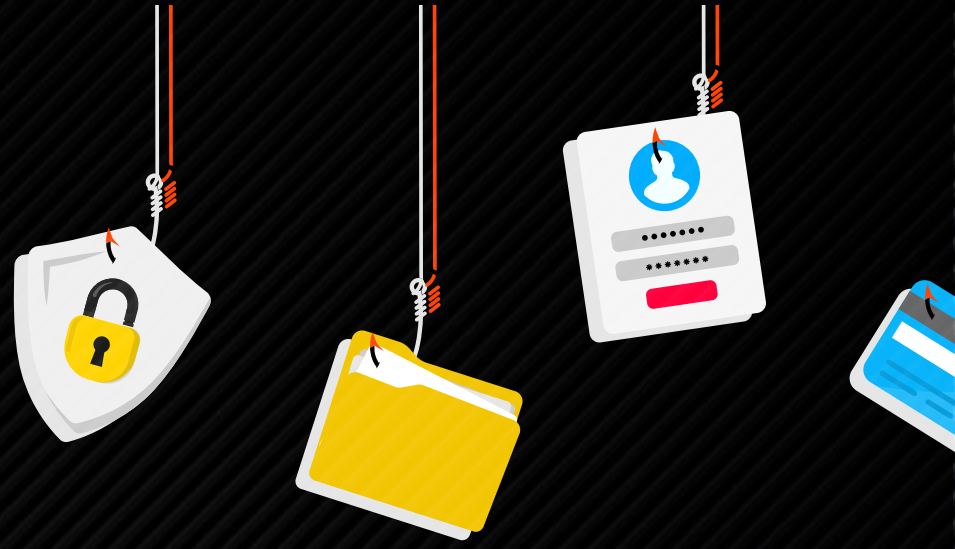
AARON BRANSON
Senior Vice President
Netsurion

TIM GUERRIERO
Information Security
Program Manager
P.F. Chang's

COURTNEY RADKE
CISO
Fortinet

TIM TANG
Director, Enterprise Solutions
Hughes

Threats



RISK ACTOR	TARGETS	OBJECTIVES	COMMON TACTICS
INSIDER THREATS - INTENTIONAL	POS, web apps, file servers / databases	Financial gain, malicious harm, competitive advantage, business disruption	Device Skimming, privilege misuse, insider info/tips
INSIDER THREATS - UNINTENTIONAL	Entire ecosystem is susceptible to unintentional harm from insider threats	None	Misconfigurations, negligence
ORGANIZED CRIME	POS, web applications, file servers / databases	Financial gain	Ransomware, Business email compromise
NATION STATE / APT	Supply chain, critical infrastructure, brand persona, people	Economic, political, military, and commercial Instability, Industrial espionage	Ransomware, IP Theft, Social media impersonation/ manipulation
OPPORTUNISTIC	Low hanging fruit, easy targets as they are available	Personal gain, validation, fun, boredom	Vulnerability exploits, network snooping, malware packages
HACKTIVIST	Websites, web apps, file servers / databases	Org retribution, fame & publicity, “cyber warrior”, positive/negative information disclosure, propaganda, personal preference imposition	Denial of Service, Botnet, Website defacement, social media hijacking

PREVENTION BEST PRACTICES	NOTES
Zero-trust model, Internal Segmentation, Cloud Access Security, RBAC, Fraud prevention training	Corporate employees, 3rd party, ex-employees
Configuration management, Robust change management, Cloud workload protection, User & Environment Behavior Analytics (UEBA)	Corporate employees, 3rd Party
Next-generation firewall (NGFW), Zero-trust model, internal segmentation, XDR (eXtended Detection & Response), backups, threat intelligence & hunter programs, brand reputation management, dark web monitoring	
Next-generation firewall (NGFW), Zero-trust model, internal segmentation, XDR (eXtended Detection & Response), backups, threat intelligence & hunter programs, reputation management, dark web monitoring	Risk assessment, asset management, XDR (eXtended Detection & Response), Anti-phishing, Identity management, Security Awareness (Supply Chain - vector, not actor)
Perimeter security, Internal Segmentation, XDR (eXtended Detection & Response), Vulnerability management, Configuration Management	“Script kiddies”, “malware as a service” - Patching and changing defaults is step #1
Web application firewalls (WAF), Cloud workload protection, Identity & Access Management Programs (IAM)	

The Threat Lifecycle

The first lens through which to consider your security operations is by phases of the **Threat Lifecycle** and ensuring you have substantive security controls at each.

PRE-BREACH

PREDICT THE THREAT

This stage of the lifecycle includes security controls aimed at identifying and prioritizing gaps in security and vulnerabilities that put you at risk for a security incident. These measures include:

- **VULNERABILITY MANAGEMENT:** Includes cyclical processes and appropriate technology necessary to scan networks and software for vulnerabilities, and prioritizing and mitigating such as closing open ports, patching outdated software, and addressing misconfigurations.
- **THREAT INTELLIGENCE:** Includes continual collection, analysis, and dissemination of information from multiple sources that in aggregate provide a thorough understanding of the threat landscape. Threat Intelligence Platforms (TIPs) should leverage both global, local, and industry-specific threat intelligence to inform a Security Operations Center (SOC).
- **APPLICATION CONTROL:** A security technology that, along with continual management, blocks or restricts unauthorized applications from executing.

PREVENT THE THREAT

This stage of the threat lifecycle has historically been an area where organizations over-invest in hopes of a silver bullet. More realistic is a mindset that perfect prevention is not possible, with the goal being to prevent as much as you practically can to give your detection and response efforts a fighting chance. Prevention controls have matured greatly from the old days of deploying a firewall and antivirus. While these mainstays have been modernized and are still standard, today's threat landscape demands additional controls such as:

- **ENDPOINT PROTECTION:** While many permutations of endpoint protection platforms (EPPs) exist, it is important to go beyond signature-based antimalware and implement human supervised Machine Learning (ML) technology that can prevent advanced attacks such as Fileless Malware, Ransomware, and Unknown or Mutating Malware. Also, ensure coverage of your network systems, operating systems, and device types.
- **THREAT HUNTING:** Proactively investigating early-stage attacks by leveraging threat intelligence and monitoring security events throughout the network. This activity requires security experts to look beyond the obvious and consider dormant malware, suspicious user behavior, and signs of "Low and Slow" cyber attacks in which the threat actor is considerably harder to detect until after the damage is done.
- **REDUCING FALSE POSITIVES:** More of an outcome than an activity, but in today's world of digital transformation leading to very noisy events, an all-too-common issue is cybersecurity analyst burnout caused by chasing down false positives and risking the eventual lapse of recognizing a real threat. Effective EPP coupled with finely-tuned ML-based Security Information and Event Management (SIEM) results in more blocked attacks and more contextualized alerts worth analyzing and remediating.

B R E A C H

Reconnaissance Weaponize Delivery Exploit

The Threat Lifecycle follows what is commonly known as the **Cybersecurity Kill Chain** and can be simplified as Pre-Breach, and after the point of "exploit" in the kill chain and Post-Breach. Within the Pre-Breach half of the Threat Lifecycle, ensure you have security controls that focus on 1) predicting threats and 2) preventing threats.

POST-BREACH

DETECT THE THREAT

Inevitably, an advanced persistent threat (APT) will find its way around the latest and greatest Predict and Prevent controls. At this time, the moment of exploit, the race is on to detect the malicious activity as quickly as possible. Mean Time to Detect (MTTD) is the average time it takes to discover a security threat or incident. To minimize your MTTD, consider these security controls:

- **MANAGED SIEM:** Security Information & Event Management platforms are the backbone of a security operation – ingesting as much of the logs and event data your network has to offer, normalizing it, analyzing it, and correlating seemingly disparate activities, resulting in priority-based alerts. It's a big job and requires a team of experts to prevent a SIEM software investment from becoming "shelfware". For most, a cloud-based, co-managed SIEM offers the best balance of maintaining desired in-house control while not drowning your staff in deployment, tuning and administrative tasks.
- **INTRUSION DETECTION:** A system that specifically monitors for malicious activity or policy violation. It's important to be aware of two classifications: Network-based IDS (NIDS) that monitors network traffic and Host-based IDS (HIDS) that monitors operating system files.
- **BEHAVIOR ANALYSIS:** A process and technology that specifically targets patterns of human behavior and detects anomalies in those patterns that may indicate compromised credentials or other threat – an individual logging in from a geographically unusual location, a user accessing a system never before accessed, multiple failed login attempts, an escalation of user privileges, etc.

RESPOND TO THE THREAT

Hand-in-hand with detecting the threat, this stage is about effectively and efficiently mitigating the threat. Mean Time to Respond (MTTR) is the average time it takes to control and remediate a threat. To optimize your MTTR, consider these controls and capabilities:

- **SECURITY ORCHESTRATION & AUTOMATED RESPONSE (SOAR):** Sometimes a separate technology, sometimes a feature of the SIEM platform in place, SOAR enables the automation of routine remediation steps and orchestration of tasks between systems such as between a SIEM and an IT helpdesk ticket system.
- **INCIDENT RESPONSE (IR):** An incident response plan is a common element of a security operation playbook that defines precisely how the security practitioners are expected to act in the case of various incident types and levels. When working with a Managed Security Service Provider (MSSP) or your own internal SOC, the Incident Response Playbook should be fully defined and frequently reviewed.
- **FORENSIC INVESTIGATION:** Once the immediate threat is contained, forensic investigation procedures focus on a deeper dive into the root cause, potentially uncovering more related threats, and identifying a plan to loop back into better prediction, prevention, and detection of such attacks.

Install | Command & Control | Action on Objectives

Controls

DEFENSE-IN-DEPTH MODEL

In addition to considering the Threat Lifecycle and security controls to address each, the second lens through which to inspect your cybersecurity controls is by the layers of assets you must protect and the measures by which each is secured. The Defense-in Depth model is a means by which you can ensure your security operations are comprehensive in attack surface coverage.

By forming a matrix of what you are protecting (Defense-in-Depth) and when you are protecting them (Threat Lifecycle), you can develop a comprehensive set of security controls for your security operations.

Identify Critical Assets

IN-STORE ASSETS

- POS and Online Ordering Systems
- Operational Systems (back-office PC, digital menu boards, kitchen display screens)
- Other Systems (DVR/Camera, Wi-Fi, etc.
- iPad - Tablets

CORPORATE ASSETS

- Support/Administrators machines
- Customer Data
- Employee Data

Data Security

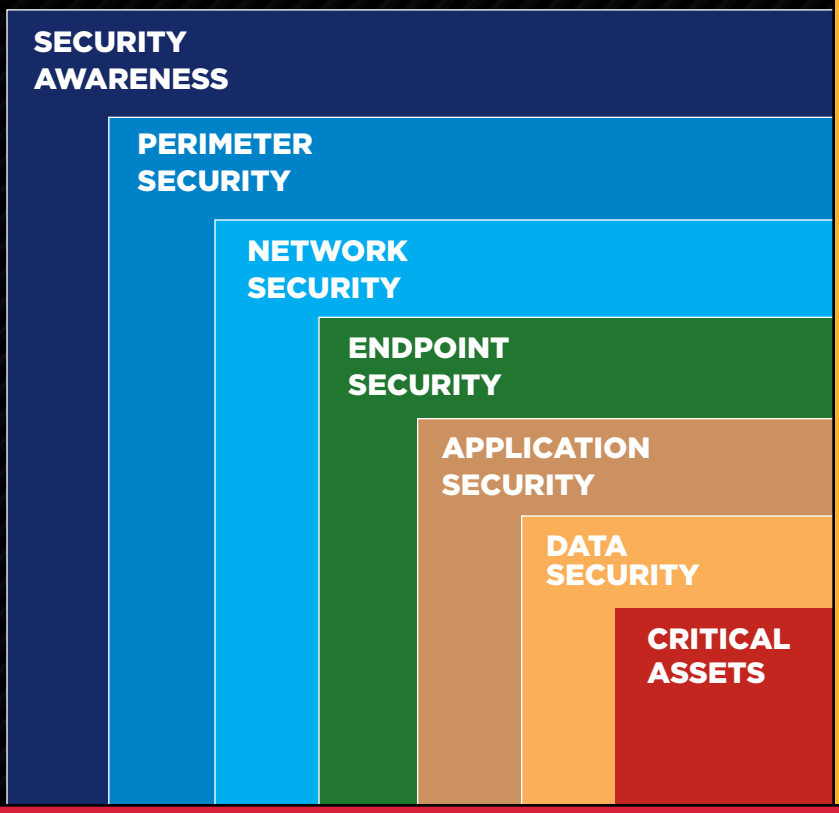
- EMV/P2PE
- Third-Party App proof of data encryption or data security best practices

Application Security

- In-house application Dev pen testing
- Expect Third-Party Apps to provide evidence of pen test

Endpoint Security

- EPP on the POS systems - can the brand add EPP to the POS Server? If locked down, has the POS Provider embedded EPP?
  - EDR - Endpoint Detection and Response



Prioritization and Implementation

- Can be daunting for smaller brands or franchisees
- If unsure, start with PCI DSS but don't stop at PCI DSS
- Identify business critical assets (above) and work through defense-in-depth layers
- Risk assessment by third party

Network Security

- Flat network: Must have stringent firewall configurations and rule-base
- Segmentation: Separate the POS, Back Office LAN, Guest Wi-Fi VLAN, DMZ for IoT devices

Perimeter Security

- NGFW, IDS w/ regular review of configurations - remove no longer needed app access or user access
- Expert monitoring on regular basis for user or entity behavior anomalies, rogue devices
- Log management: local devices and firewall, file changes, URL communication, protocol usage

Security Awareness Training

- In-Store: Safe credit card handling for PCI DSS, POS Inspection and tampering
- Corporate: Security awareness, phishing, user account and password hygiene
- Administrators Training

Outsourcing Opportunities

SOC - Security Operations Center

NOC - Network Operations Center

Tier 1 support

Architecture

RACI Matrix for Restaurant Cybersecurity

	RESPONSIBLE	ACCOUNTABLE	CONSULTED	INFORMED
C-SUITE		X		
MANAGEMENT	X			
OPERATIONS/ SUPPORT	X			
EMPLOYEE			X	
CUSTOMER				X

ACTIVITY	INCIDENT MANAGER	INCIDENT COORDINATOR	INCIDENT ANALYST	INCIDENT OPERATOR	SERVICE DESK AGENT	SERVICE DESK MANAGER	USER
Incident Logging & Categorization							
Incident Assignment							
Incident Investigation and Diagnosis							
Incident Resolution and Recovery							
Incident Review and Closure							
Incident Escalation							
SLA Monitoring							
OLA and UC Monitoring							
Complaint Handling							

ROLE	DESCRIPTION	STAFFING (INTERNAL VS. OUTSOURCING)
ENGINEER	Responsible for build-out, deployment, and maintenance of information security systems. Maintain security lifecycle. Works with Architect on development of IS systems and responsible for deployment and ongoing life-cycle.	Generally a full-time internal resource that is sometimes augmented by external service provider
ANALYST	First to respond to security events and incidents. The core role of the SOC as defined by analyst hierarchy.	
TIER 1	Routine log and alert analysis. Validation of security incidents and proper escalation. Responsible for day-to-day security tool monitoring and configuration management.	Due to the nature of the role, this position is generally outsourced or maintained via a non-FTE and/or contractor methodology. This is a24x7 role though we are now seeing this role being automated and/or eliminated in some cases via the use of tools such as AI-augmentation / AI-analyst
TIER 2	Responsible for addressing escalated incidents as identified by Tier 1 analysts. Identification of threat exposure and affected systems. Carries out containment and remediation strategies as well as recovery and root cause analysis. Recommends changes and updates rule-sets and IOCs (indicators of compromise).	May be internally staffed, augmented, or wholly outsourced based on budget, maturity, or individual needs of the organization. This can be 24x7, 9x5, or engagement as part of the incident management escalation process.
TIER 3 (INCIDENT RESPONSE)	Handle critical incidents. Responsible for communication to leadership and ensure consistent operations of security tools and services. Conduct assessments on efficacy and carry out vulnerability assessments, penetration tests, and table-top exercises. May serve as incident response manager.	Staffed as needed / according to incident prevalence and company risk posture. Seasoned/veteran analyst that many times is internal FTE or dedicated MSSP analyst.
THREAT HUNTER	Active cyber defense activities to detect and isolate advanced threats in the environment	Generally part of MSSP offering and is purposefully external to the company.
ARCHITECT	Create framework for security operations and responsible for development of policy, procedure, and requirements. Assists engineers with design/build phase and responsible for overall IS strategy creation.	Generally dedicated internal FTE though may be part of consulting services and/or service provided by MSSP.
CISO	Executive Cyber Security leader responsible for setting strategy and direction for security functions within an organization.	Executive-level internal position though vCISO (virtual CISO) services are becoming more common especially in smaller organizations without robust internal security offerings.

Restaurant Technology Network

join. share. thrive.

RTN Vision

In an industry built on service and entrepreneurial spirit, purpose-built technology fuels success. The Restaurant Technology Network aspires to help restaurant professionals and solution providers work together to solve problems large and small and inspire bold ideas for the future.

Join Us

If you have a vested interest in the restaurant technology industry, join us. Collectively, our members shape the industry by creating and disseminating technology standards and technical guidance to benefit members. Through our cornerstone virtual think-tank workgroup meetings, our members solve industry challenges and prosper inside a unique, collaborative environment.

+ VIEW OUR MEMBERS

www.restauranttechnologynetwork.com