Recommended Baseline for Information Security Controls

Prepared for members of the Meat Institute by:

Ricardo Lafosse – CISO The Kraft Heinz Company

Roberto Gutierrez – CISO OSI Group

Meat Institute

Nourishing Today
Sustaining Tomorrow

Top Areas to Focus

Backup/Restore

Vulnerability Management / Patching

Visibility, Segmentation & Logging

Email / Web protections

Incident Response / Tabletop Exercise

Endpoint Security

Access Management / Local Admin

Awareness

Backup/Restore

GOALS

Backup assets

Capable to restore assets in a timely manner

Protect backup infrastructure

SCOPE

Start with critical assets

Expand based on your comfort

PRO TIPS

Identify critical assets – Align with the Business

Routinely perform restores

Perform full system restores on quarterly basis

Protect your backups

Understand the time to restore

Backup/Restore Pro Tips

Identify Critical Assets

Start with IT
Obtain executive buy-in for business input
When in doubt backup everything you can

Full System Restore & Resource Needs

Choose a new system to restore each quarter (must be from the ground up)
Priority of servers to restore is key, so document
Standby capacity to restore

Routinely Perform Backups/Restores

Set a backup schedule (mix differentials & full)
Perform file and folder level restores on a set interval (no longer than a month)
Consider Immutable/Encrypted Backups files

Timing

Document time to restore a full system
Document in run books and IR Plan
Choose a Backup strategy aligned with acceptable timeframes.

Incident Response / Tabletop Exercise

GOALS

Key response actions to known incidents

Decision / x-process points & call tree

Roles & Responsibilities

Communications

SCOPE

Relevant business disruption scenarios

Global / Regional / Local Processes & Technology

Applicable threat/risk vectors

Crown jewels

PRO TIPS

Share and rehearse - Protect it but make it available

Know/work with your partners – Retainer/SLAs (IR responder, Insurance, Legal counsel, negotiators, etc.)

Living document/process. Update it

Understand your team’s skills

DR & BCP

Incident Response / Tabletop Exercise Pro Tips

Share and Rehearse

It must be known by the personnel involved in the recovery process

Tabletops would help personnel to familiarize with the response roles and responsibilities

Continuous process

Update the IR and DR plans frequently

Priority of servers to restore is key, so document

Consider communications SMEs

Know your team and partners

Who is who and what they do. When to call them in?

IT team skills must be known before needing them

DR & BCP

A defined DRP will help to shorten the time to recover

Consider time consumed by forensics and other processes

Business must/should operate in manual mode

Vulnerability Management / Patching

GOALS

Reduce attack vectors

Identify exploitable weaknesses

Continuous improvement and prevention

Know your environment

SCOPE

Anything with an IP address

Global / Regional / Local by Technology

On-prem, Cloud & Third Party

PRO TIPS

Never ending process

Look out for trends

Partner with the right tool

Be aware of tool/vendor mutations

It is a team effort

Vulnerability Management / Patching Pro Tips

Never ending

Vulnerabilities everywhere – understand your environment
Scan, assess, patch, repeat – know your exceptions
Identify trends in IoCs and track those

Patch

Patch, patch, patch
Work with and push vendors or isolate/segment technologies
Dedicated resources (if possible)

Tooling and Partners

Many tools out there, find the one that would work for your environment and team
Understand your vendor strategy and progression

Team Effort

Is not an IT Security process
Work with your IT team and business
Track and report

Endpoint Security

GOALS

First line and continuous defense (In/Out trusted networks)

Detect and act on unknown, unauthorized or malicious actions

Identify key IoCs

SCOPE

Protect everywhere

- Ideally anything with an IP address

OT / IoT / IIoT – push boundaries

Mobile / Tablets

PRO TIPS

Dedicated resources and/or managed service / Team effort

Continuous monitoring and alerting

Base protection controls (Up to date OS, Encryption, strong authentication, access control & hardening)

Response capabilities (EPP, EDR, XDR)

Consistency & Continuous deployment

Endpoint Security Pro Tips

Team and reach

Requires committed resources to deploy & maintain
Cover infrastructure everywhere - w/exceptions
Look for unknown environments & devices
Best done by a dedicated/skilled team

Response

Response capabilities are a must
Application, DLP and data privacy protections Policies

Monitoring and Alerting

Centralized
X-check with other tools
Enrich with threat intel – integrate SOC/SIEM/SOAR
Assess/Correlate real-time IoCs

Continuous Process

Ongoing management/responsibility
Hardening, encryption, limit local admin
Shared responsibility with the user- are they aware?
Not just an AV

Visibility, Segmentation & Logging

GOALS

Protect/Secure all

Look for what you can’t see -is shadow IT a thing?

Segment critical networks serving core operations or services

Log applicable data and use to assess, identify and alert

SCOPE

See everything (moving target)

Segment critical networks

Log what is meaningful and can be acted on

Keep enhancing/increasing

PRO TIPS

SIEM/SOC/SOAR great to have - must be manageable

Partner with appropriate third parties if no internal resources available

Segmentation based on standards – pragmatic

No need to Log everything

Visibility, Segmentation & Logging Pro Tips

Visibility

X-reference scanning and inventory systems
Discovery is a never-ending process / understand responsibilities
Assess relationships between networks/devices

Logging

Start small and grow as the process mature
Logs must be meaningful
Enrich and use to alert

Segmentation

Based on standards but tailored to your own environment
Require efforts from both business and IT
Once in place, control & monitor access/traffic

Other

Find a partner where internal resources are not available
Evaluate as many prospect partners and solutions as possible

Access Management / Local Admin

GOALS

Enforce least privilege

Multifactor authentication (MFA) is key

User lifecycle basics (onboarding/offboarding)

SCOPE

Enforce MFA to external systems (system by system)

Employees, contractors, and other 3rd parties must be included to be effective

PRO TIPS

Ensure new users only have the access required (group-based rules)

Modular approach to MFA

Document termination processes

Audit your own program

Access Management / Local Admin Pro Tips

Ensure new users only have the access required (group-based rules)

Identify common groups of user access and expand
Communication and executive buy in are key
Recertify access at a given internal (quarterly, yearly, etc)

Document termination processes

Collaborate with HR and understand process
Ensure termination of ID disabled ALL access
Gradually move to automation
Document automated and failback manual processes

Modular approach to MFA

Identify single MFA service (one user experience)
Email and/or VPN are solid starting points and expand
Start with friends and family for feedback

Audit your own program

Evaluate the effectiveness of your controls
User/group access reviews
Always build upon prior successes

Email / Web protections

GOALS

Protect users from common threats

Provide multi-layer controls for email/web

Train users to be vigilant when on the web

SCOPE

Layer email controls in a modular fashion

Implement web controls at the host and network

PRO TIPS

Deny risky attachment extensions in email

Implement DKIM and SPF (bonus points for DMARC)

Implement web filtering

Ensure hosts have endpoint security

Email / Web protections Pro Tips

Deny risky attachment extensions in email

Start with risky extensions that are easy (e.g. .exe,.vbs)
Build upon the list with user communication (e.g. macros for excel)
Monitor for efficacy and tuning

Implement web filtering

Implement host based or network-based web filtering
Start with blocking common categories (e.g. gambling) and expand from there
Develop exception process

Implement DKIM and SPF (bonus points for DMARC)

Test DKIM and SPF on low traffic domains and understand how they work
Marketing, sales, and email team collaboration is key
Perform end user communication prior to switching on

Ensure hosts have endpoint security

Validate end point security is installed and up to date
Ensure that any exclusions are for business applications
Integrate end point security agent with email client

Awareness

GOALS

Educate end users on security best practices

Focus on using strong passwords and social engineering tactics

Continuous training not once a year

SCOPE

Decide on platform to communicate end users

Contractors and non-employees accessing your resources should be included

PRO TIPS

Perform in-depth annual training

Monthly newsletters/advisories

Perform phishing exercises

Develop workshops for passwords/social engineering

Awareness Pro Tips

Perform in-depth annual training

Ensure content is relevant and easy to understand
Training should highlight key areas of your program
Great opportunity to encompass any required regulatory training

Perform phishing exercises

Perform monthly/quarterly phishing tests to various segments of your community
Track click rates and reinforce with additional training

Monthly newsletters/advisories

Ensure content is easy to understand
Ensure content is relevant to your month’s theme or threats
Highlight actionable takeaways

Develop workshops for passwords/social engineering

Develop workshops for constructing strong passwords
Highlight the tactics used for social engineering