HALOCK®

Risk Management Program

Demonstrate Reasonableness to ALL interested parties

Satisfy Compliance Obligations

Defines Line of Acceptable Risk

Improves Decision Making

Access to Intellectual Property to build Security Program

Justifies Budget Requests

Virtual Security and Risk Staff (Access to industry experts)

Industry-Specific Threat Modelling

# How to Calculate Risk with Best-in-Class Risk Criteria

Likelihood

Estimate Likelihood with

HALOCK'S Industry Threat (HIT) Index

How prepared are you for the most common threats?

HALOCK's HIT Index analyzes thousands of cybersecurity incidents to find patterns of threats in different industries.

By mapping threat commonality to control maturity, we can estimate how likely an incident will be caused by which threat.

THREAT COMMONALITY — 78%

CONTROL MATURITY — Measured & Corrected

LIKELIHOOD

1
2
3
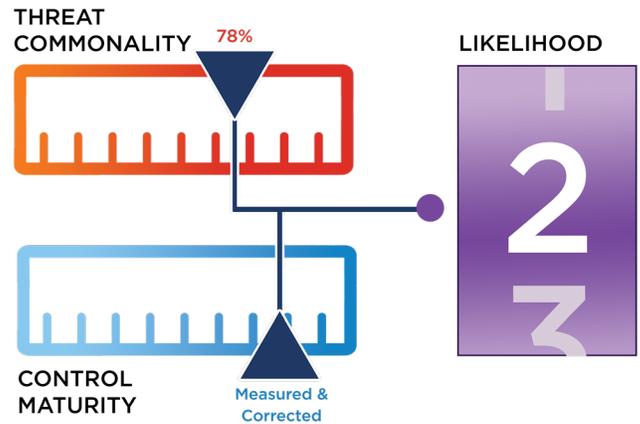
X

Impact

Estimate Impact With

Duty of Care Risk Analysis (DoCRA)

Is your risk reasonable?

Risk assessments should consider impacts to your business, your purpose, and the harm you may cause others due to a cybersecurity event.

With DoCRA, you will demonstrate reasonable risk - that you put the public's safety on the same level as your own.

= Risk

Halock's Risk Management Program

offers a comprehensive and streamlined approach to define reasonable security, prioritize investment, and establish alignment across your organization. As part of the program, the team provides baseline analysis and retainer services with access to our intellectual property resources. You have the option to get an integrated risk management GRC tool – Reasonable Risk, that would further enhance your security program.

Components to Risk Management Program

BASELINE ANALYSIS AND REMEDIATION PLANNING

Develop Risk Criteria
"CARD"

Baseline Analysis & Treatment Plan

Develop Remediation Roadmap

RETAINER SERVICES

Develop Key Indicators

Remediation
Policies, training, Incident Response (IR), Audit, Implement Controls

Execution Dashboard & Reporting

INTELLECTUAL PROPERTY ACCESS

RISK ASSESSMENT TOOLS AND METHODS

RISK ASSESSMENT RUN BOOK TOOLS

RISK ASSESSMENT EXECUTIVE REPORTING TOOLS & TEMPLATES

BUDGET JUSTIFICATION TOOLS & TEMPLATES

POLICY TEMPLATES (NIST, ISO, PCI)

SECURITY AWARENESS TRAINING CONTENT

QUARTERLY BRIEFING

INTERNAL AUDIT SCRIPTS AND PROCESS

THIRD PARTY PROGRAM COMPONENTS AND TEMPLATES

ISMS RUN BOOKS (ISO 27001)

PCI MAINTENANCE RUN BOOKS

INCIDENT RESPONSE PLAN TEMPLATE (NIST 800-61 BEST PRACTICES)

INCIDENT RESPONSE PLAN VIDEO TRAINING

INCIDENT RESPONSE SERVICE LEVEL AGREEMENT (SLA)

INCIDENT RESPONSE RUNBOOK TEMPLATES

INCIDENT RESPONSE TABLETOP EXERCISE TEMPLATES

FIRST RESPONDER TOOLKIT

FIRST RESPONDER TRAINING CONTENT

VIDEO AND WHITE PAPER SUBSCRIPTION CONTENT (COMING SOON)

THREAT DATA (HIT INDEX)

SECURITY AWARENESS POSTERS
TIPS & TRICKS

Better Decisions through Better Risk Criteria from DoCRA

Risk#	Threat	Likelihood	M	Obj	Obl	Risk
A	Web attack	5	3	2	4	20
B	Insider abuse	4	2	4	3	16
C	Ransom-ware	4	4	4	3	16
D	Lost device	3	5	3	3	15
E	Malware	3	3	4	4	12
F	Social Engineer	3	1	2	2	6
G	Mis-delivery	2	2	3	1	6
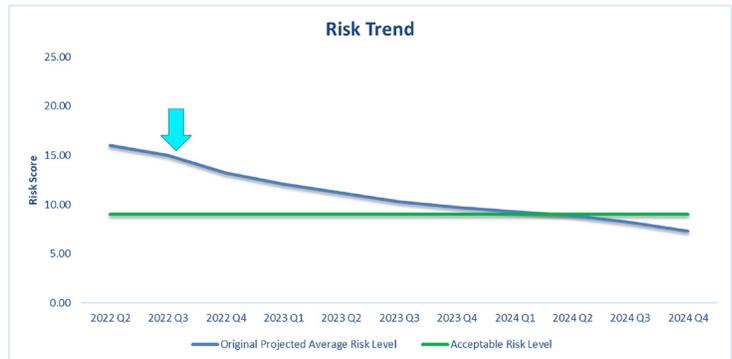
Risk Trend

Risk#	Threat	Likelihood	M	Obj	Obl	Risk
A	Web attack	5	3	2	4	20
B	Insider abuse	4	2	4	3	16
C	Ransom-ware	4	4	4	3	16
D	Lost device	3	5	3	3	15
E	Malware	3	3	4	4	12
A	Web attack	2	3	2	4	8
F	Social Engineer	3	1	2	2	6
G	Mis-delivery	2	2	3	1	6

Risk Trend

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173

847-221-0200

halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Reasonable Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, and Security Engineering and Products.

About the DoCRA Council

The DoCRA Council is a not-for-profit (501(C)(3)) organization that authors, maintains, and distributes standards and methods for analyzing and managing risk. The DoCRA Council is comprised of member organizations that require standards of practice in risk analysis and risk management, and who therefore have an interest in the methods used for analyzing risks and safeguards that reduce risk.