Review Your Risks
Before Getting Cyber Insurance

Cyber insurance companies consider many factors about a company before providing coverage; risk is the most prominent. The higher the risk, the higher your premium. Assess your security and risk profile at the start of your cyber insurance process.

Are You Prepared to Answer Details About Your Cybersecurity Program?

Multi-Factor Authentication (MFA)	*Does your organization use MFA?* Probably the most important security control is the application of multi-factor authentication (MFA) to protect your company's data, especially for mission critical data systems and data stores. With MFA, stolen credentials are useless if the threat actor doesn't also have the authentication device used for access.
Backup Program & Data Management	*Does your organization have a business continuity program (BCP) in the event of a breach or attack? Do you have a current data inventory of how and where your sensitive data is managed?* Backing up key data regularly and conducting period tests to demonstrate the ability to restore that data are a key part of any rigorous disaster recovery program and your best control to minimize downtime in the event of a ransomware attack.
Implement Principle of Least Privilege (PoLP)	*How do you manage employee access to your network, data, and controls?* Reduce the amount of accounts that have full permissions to operating systems and applications such as Windows Active Directory domain administrators or accounts created for application access to windows domain and system resources, commonly referred to as service accounts. Create accounts that have only the access needed to perform the function required within an operating system or applications.
Data Minimization Program	*How do you determine how much information you should manage, to be in compliance, and dispose of data that is not needed?* Effective reduction of data that is either redundant, obsolete, or trivial (ROT) is an important factor to reduce the amount of sensitive data that is at risk, as we saw in the California Pizza Kitchen data breach. Prompt erasure of personal data which is no longer needed for the purposes it was originally collected is also a compliance requirement of Article 17(1)(a) of GDPR. Hackers can't access sensitive data that is no longer there.
Prompt Application of Patches	*How do you manage updates and patches with your network and systems?* The ability to demonstrate a program of prompt application of software and operating system patches and security updates can also reduce risk. A delay of a mere four days in applying a patch for the Log4j vulnerability was all it took for ONUS to be impacted by a ransomware attack in December 2021.
Endpoint Detection and Response (EDR)	*How do you protect your endpoints such as mobile phones, laptops, IoT devices from threats?* Implementation of an EDR security solution that continually monitors and collects data regarding your connected devices and applies rules-based automated responses to respond to cyber threats.
Email Security and Configuration	*How are you securing your emails from phishing or threats?* Having a program to keep spam and malware filters current will reduce phishing attempts getting to intended email targets, reducing risk.
Mobile Device Management (MDM)	*How are you securing your emails from phishing or threats?* Implementation of MDM methodologies and toolsets can minimize the risk related to mobile devices, especially bring your own device (BYOD).

Routine Cyber Training Security Awareness Incident Response First Responder	*Do your teams know your policies, what are the latest hacking techniques and how to determine if you are under attack?* A comprehensive training program for all employees, with regular intervals to reinforce training principles and spot training as needed to address newly identified risks, is another important security control for companies to have.
Policies and Procedures Documentation	*Does your organization have current, documented, and disseminated security policies and procedures to manage your data and network?* Another way to reinforce security best practices is up-to-date policies and procedures associated with the use of technology within the company, especially with regard to credentials and passwords.
Incident Response Plan (IRP)	*Is your organization ready for a cyber threat and attack? Are your teams ready to respond – what to do, who to contact, what to communicate? Do you have a Written Information Security Policy (WISP)?*
Penetration Testing & Vulnerability Scanning	*How are you regularly verifying your security controls are effective for your changing business environment?*
Compliance HIPAA PCI DSS Privacy	*Are you currently in compliance with your organization's latest regulations?* *How do you maintain your compliance requirements?*
Third-Party Risk / Vendor Risk	*Do your consultants and vendors have access to your data and networks?* *How do you ensure they are practicing the same security protocols as you do?*
Penetration Testing	Insurance underwriters expect to see regular pen testing performed by a 3rd party. Pen testing should not be confused with automated vulnerability scanning. While both may find vulnerabilities, a pen test is simulating what a motivated threat actor may accomplish. Pen testing is viewed as the ultimate control effectiveness test.
Web Application Firewalls (WAF)	Required by PCI DSS, a WAF is increasingly seen as table stakes for organizations that have a big on-line presence. It should be noted that a WAF is a not a substitute for secure coding practices (OWASP v4), but can slow down hackers by blocking many of the common attempts of hacking web applications.
Duty of Care Risk Analysis (DoCRA)	*How do you manage risk?* The largest cost to a breach, according to Netdiligence Reports, is liability (regulator fines, class action lawsuits and attorney fees). Organizations that can demonstrate they have a Duty of Care-based Risk Management Program can reduce their overall risk to themselves and cyber insurance carriers. An effective risk management program tells interested parties, including underwriters, you are on top of the new risks and associated risk treatments. Core components of a defensible risk management program include • Risk scoring criteria that includes impacts to those outside the organization • Define an acceptable level of risk (acceptable to all parties) • Define a process to determine the reasonableness (or burden) of remediation efforts • Document your calculus (risk register) • Manage Remediation (program management) • Regular updates to the risk register (at least annually)

Be ready for the underwriters. These controls are your best defense against the rising costs of cyber insurance, and they are key indicators for cyber insurance carriers to assess risks that influence insurance premiums.

What are the Top Threats in Your Industry?

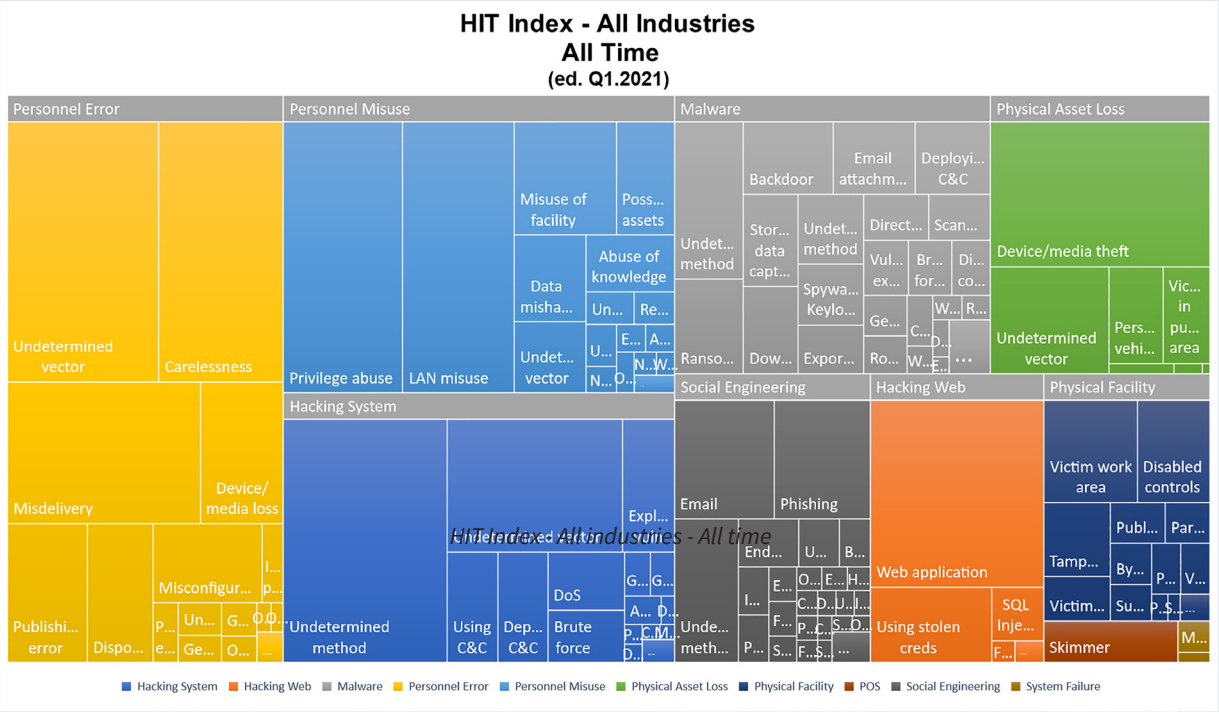
Secure & Prepare Your Organization through Industry Insight.

HALOCK's Industry Threat Index (HIT) is a model for estimating the most likely (and least likely) ways your organization will be hit by a cybersecurity or information security attack. We review the deep data in the Veris Community Database and find patterns in attacks that affect different industries. Because industries use systems and information in certain ways, each organization in an industry experiences similar patterns of breaches, leaks, and security failures.

Manage Your Risk

Compare the HIT Index information to the strength of your controls that would prevent or detect those attacks. Estimate the most and least likely ways your organization will suffer a cybersecurity or information security incident.

Schedule a call to discuss the HIT Index and how it can support your security and risk program.



Managing Your Risk

Risk Management Aligning Your Organization's Mission, Objectives, and Obligations

Risk is always a part of your cyber strategy. It evolves based on your environment. It could be calm one moment, then a disastrous storm the next. The key to managing risk is to continually take care of your critical business areas and all interested parties.

But how do you manage the needs of many with different priorities?

Risk management programs must consider all perspectives and impact. Not only do you identify risks and likelihood, but you also must establish safeguards to protect against those risks. Regulatory requirements tell us security controls should be 'reasonable', and organizations are challenged to define their duty of care for the their specific working environments.

Justify budget requests

Defining the Line of Acceptable Risk

Risk Management as a differentiator

Lower Cyber Insurance Premiums

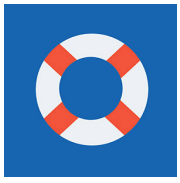
Compliance Drivers Requiring risk management

Align the Business Needs with Other Parties (regulators, insurance, clients)

Enable the Organization to meet its Duty of Care (reduce organization liability)

Manage Incoming Client Security Questionnaires

Protect the Mission and Increase the Valuation



Meet Injunctive Relief Measures

Establish reasonable security through the Duty of Care Risk Analysis (DoCRA). **Duty of Care** requires that organizations demonstrate they used controls to ensure that risk was reasonable to the organization and appropriate to other interested parties at the time of the breach. This approach enables users to:

HALOCK is uniquely positioned to help you develop 'reasonable security' that accomplishes all this. And offer you a risk calculus that is absolutely defensible.

Schedule a review of your risk profile to define ***reasonable security***.

HALOCK

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200
halock.com