WHITE PAPER

Cybersecurity Risk Assessment

Understand Your Risk Exposure

THRIVE℠

Where Does Your Cybersecurity Stand?

Cybersecurity risk management applies to business entities in every vertical. Whether you're in finance, healthcare, education, or beyond, it is vitally important to know your organization's security posture on an ongoing basis. Especially when signing up for a cybersecurity insurance policy, insurers need to know where an organization's risk profile currently stands and the steps they're taking to proactively mitigate cyber risk on an ongoing basis.

A Cybersecurity Risk Assessment involves reviewing a company's technology infrastructure and related processes to identify potential vulnerabilities and to verify that controls are put in place to minimize organizational risk. It evaluates cybersecurity posture and currently deployed solutions against the Center for Internet Security's (CIS) 18 identified control areas. This comparison provides a comprehensive snapshot of a company's current risk profile to understand current state and to build a strategic roadmap. Lead by one of Thrive's (ISC)2 certified Strategic Consultants, a Cybersecurity Risk Assessment (CRA) reviews all existing policies, controls, and compliance oversight to improve an organization's cybersecurity posture.

No matter your needs or those of your clients, Thrive's evaluation standards create a robust foundation to support proactive cyber risk mitigation. One-size-fits-all solutions for cybersecurity protection simply do not provide a comprehensive approach to seal every potential vulnerability in your organization's security program. Overlooked processes such as a lack of due diligence on 3rd party business partners can put your business and client's data at risk. With so many variables at play, a security program that aligns with a formal comprehensive security framework, such as CIS v8, protects your organization's data, brand image, and even reduces the chance of potential future legal action.

Reinforcing Your Cybersecurity Insurance Policy

It seems straightforward to think, "I have an insurance policy, that should be enough to cover me - right?". In some sense, yes - cybersecurity insurance can be a very important tool to assist your organization in the event of a damaging cyber attack. Stopping an attack from ever happening or taking hold is arguably much more important than picking up the pieces after a disastrous infiltration event.

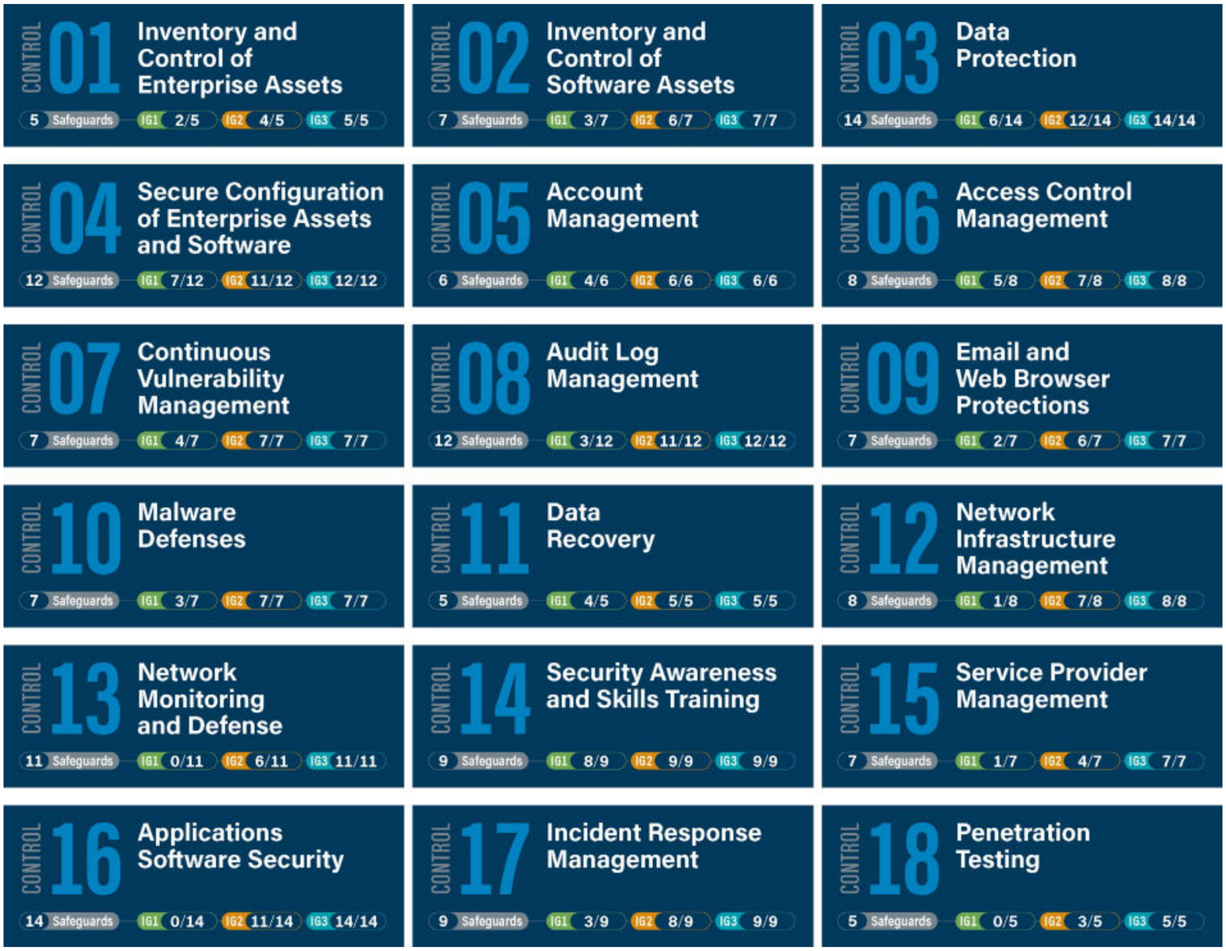
While an insurance policy can help you cover the costs of restoring lost data and resuming business as usual, it cannot repair the damage done to your business' brand reputation and client relationships, nor can it recall your or your clients' data that was already leaked to the dark web. Cybersecurity insurance is a single component of a comprehensive cyber risk mitigation strategy, and is a beneficial tool to keep on hand to protect your business's brand image and assets.

What are CIS Controls?

The Center for Information Security (CIS) is a nonprofit organization with the mission to "make the connected world a safer place." They have developed sets of protocols and best practices to help individuals and larger groups protect themselves against pervasive cyber threats.

CIS Controls are a highly recommended set of prescribed actions organizations can take to establish and promote their cybersecurity posture. These controls provide specific, actionable ways to put a barrier between your data and malicious intruders. They are broken down into basic, foundational, and organizational categories, prioritized in that order. Each group of controls identifies areas of focus and recommends best practices to bring your security measures into compliance.

Most importantly, CIS Controls are compatible with other well-known frameworks such as HIPPA, NIST, and ISO 27001. This compatibility ensures that Thrive's CRA will benefit you and your clients, no matter what industry or sector you operate in.



Control		Safeguards	IG1	IG2	IG3
01	Inventory and Control of Enterprise Assets	5	2/5	4/5	5/5
02	Inventory and Control of Software Assets	7	3/7	6/7	7/7
03	Data Protection	14	6/14	12/14	14/14
04	Secure Configuration of Enterprise Assets and Software	12	7/12	11/12	12/12
05	Account Management	6	4/6	6/6	6/6
06	Access Control Management	8	5/8	7/8	8/8
07	Continuous Vulnerability Management	7	4/7	7/7	7/7
08	Audit Log Management	12	3/12	11/12	12/12
09	Email and Web Browser Protections	7	2/7	6/7	7/7
10	Malware Defenses	7	3/7	7/7	7/7
11	Data Recovery	5	4/5	5/5	5/5
12	Network Infrastructure Management	8	1/8	7/8	8/8
13	Network Monitoring and Defense	11	0/11	6/11	11/11
14	Security Awareness and Skills Training	9	8/9	9/9	9/9
15	Service Provider Management	7	1/7	4/7	7/7
16	Applications Software Security	14	0/14	11/14	14/14
17	Incident Response Management	9	3/9	8/9	9/9
18	Penetration Testing	5	0/5	3/5	5/5

https://www.cisecurity.org/controls/implementation-groups/ig3

The Steps in a Cybersecurity Risk Assessment

1. Current State Overview

Thrive first looks under the hood to assess everything your organization has at play. An CRA oftentimes requires delegate access to your organization's existing systems, and even a visit to your offices to check out any on-premise equipment and endpoint devices. During the assessment, Thrive's team reviews all three levels of controls - basic, foundational, and organizational.

Basic Controls

There are six basic controls that serve as a foundation for your organization's security posture. These basic controls ensure your hardware and software assets are being appropriately monitored, managed, and tracked to best protect from and remediate the most common vulnerabilities.

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Admin Privileges
5. Configuration for Hardware and Software on Mobile Devices, Laptops and Servers
6. Maintenance, Monitoring, and Analysis of Audit Logs

Foundational Controls

This second, and largest, group of controls build upon the foundation established by the first set of basic controls to strengthen your frontlines. Implementing these controls better protects your organization from more sophisticated - yet still quite common - cyber attacks.

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices such as Firewalls, Routers, and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Incident Response Management
18. Penetration Testing

Organizational Controls

Organizational controls establish a framework for responding to incidents and testing your systems for future threats. These controls protect your most valuable assets and act as the final safeguards and redundancies, and ensure that any vulnerabilities are not exploited more than once.

2. CIS Comparision

After assessing where your organization stands on each of the 18 CIS v8 controls, Thrive compares its findings with recommended best practices. These best practices include NextGen firewalling, overarching governance plans, and multifactor authentication (MFA) usage across logins. This gap analysis compares your organization's properly deployed protocols against those typically prescribed to improve security posture.

3. Prioritized List

As a final step during your CRA, Thrive prepares and presents a clear report that is built for both executives and tech teams alike. This review recaps the CIS v8 standards and presents them in an easy-to-read table, comparing your security posture with the most up-to-date mitigation tactics. Each area of non-compliance is then flagged with an associated level of urgency - low, medium, or high. Along with these recommendations, Thrive gives your team an approximate associated cost on the open market to bring your security position into compliance.

Do You Know Your Risk Exposure?

It is easy to tally up the protocols and procedures your organization has in place to stay protected from potential hackers. When was the last time those processes were reviewed as a cohesive system? Hackers are not picky when it comes to choosing a victim, meaning everyone is a target. If you want to take a serious look at where your security weaknesses lie and what is being done to reduce your risk exposure, a security risk assessment from Thrive can help. Understand your security posture and be better protected in the event of an attack by contacting us today.

Contact the Thrive Team

To Learn More, Contact Us Today, or Give Us a Call At:

thrivenextgen.com | info@thrivenetworks.com

1-866-205-2810

About Thrive

Thrive is a leading provider of NextGen managed services designed to drive business outcomes through application enablement and optimization. The company's Thrive5 Methodology utilizes a unique combination of its Application Performance Platform and strategic services to ensure each business application takes advantage of technology that enables peak performance, scale, and the highest level of security.