

CyberClan's Risk Management Services

Exclusively for

DUAL¹

cyberclan.com

¹ DUAL Commercial LLC ("DUAL") is a specialty program manager underwriting financial lines insurance products on behalf of various insurance carriers.

Executive Summary

The cyber insurance market has changed significantly in the last two years. Several key cyber security controls need to be in place to ensure placement or renewal and to avoid withdrawal and/or limitation of important warranties, significant increase in deductibles and decreased limits. CyberClan and our partners have identified these key controls to help our clients to understand and prepare their cyber placement or renewal application.

CyberClan's proactive and risk management services assist organizations in strengthening their cybersecurity risk posture by identifying the organization's vulnerabilities, building the appropriate security architecture, and strengthening their most effective firewall – the human one.

The objective of these specialized risk management offerings is to reduce risk by implementing security controls to protect your client's operational infrastructure from cyberattacks.

CyberClan will take a proactive approach in working with your clients and addressing all findings and vulnerabilities and improving your client's overall cybersecurity posture.



DUAL Exclusive Offerings



Offered through CyberClan

Congrats on your recent purchase of your policy. As a part of your policy, you have access to these exclusive complimentary CyberClan risk management services and are also eligible to access the following specialized services at a discounted rate.

Complimentary CyberClan Risk Management Services



2-Hour Consultation

Free consultation with a cyber expert to review your current cyber risk landscape



Complete Malware Services

Free trial, (30 days of data- 2 weeks retrospectively and 2 weeks during the service)



Cyber Security Online Education Training for Employees

A free 10-day trial of the education training.



Perimeter Security review and vulnerability baseline risk assessment



Monthly cyber security newsletter

Sent to your risk manager, detailing current threat trends.



Managed Advanced Email + Collaboration Security

Free 2-week trial of our email security.

Please contact Jane Vardzel at Jane.vardzel@cyberclan.com to learn more.





M365 Cybersecurity Assessment

Configuration Assessment and Monitoring by CyberClan

CyberClan analyzes the performance and functionality of a product in scope and compares it against its system requirements and design standards.

This assessment uncovers network and system configurations for vulnerabilities that may exist that threat actors can use to exploit the environment. Configuration Assessments are not limited to physical networks, but also extend to the Cloud.

*Available at an additional cost

CyberClan's assessment methodology includes structured review processes based on recognized "best-in-class" practices as defined by such methodologies as the ISECOM's Open-Source Security Testing Methodology Manual (OSSTMM), the Escal Institute of Advanced Technologies (SANS), the Center for Internet Security (CIS).

The Assessment is performed by CyberClan's Ethical Hackers and under the supervision of CyberClan's Senior Security Advisor

CyberClan uses the CIS Microsoft 365 Benchmark that is established as an industry best practice for security to conduct the assessment.

How it Works

The current environment configuration is tested against industry best practices

A baseline score is provided with remediations and hardening recommendations

Assessment and Review Procedures

Review Data and Flag Important Information

- CyberClan begins any assessments of procedure, policy, configuration, or documentation by reviewing all data in its entirety and completing detailed information condensing and flagging process.

Assessment of Data Against Known Best Practice

- We compare all collected data against known best practice standards
- Finally, our own in-house experts will review all recommendations and assessments, offering their own input and considerations.

Benefits of a Configuration Assessment

- Providing identification of the current network layout infrastructure
- Identifying technology within the environment that is misconfigured or missing necessary security patches
- Ultimately bolstering overall security and layout configuration of a network infrastructure



IT Rationalization Assessment

vCISO Services by CyberClan

CyberClan's vCISO team is comprised of seasoned cybersecurity executives who understand how to balance your business needs with compliance requirements, risk, and emerging threats.

Whether our team is merely augmenting a robust CyberSecOp and IT team, or providing all information security services, the offering can be tailored to your business.

Engaging a C-level executive as vCISO can help build an organization's mature security posture using CyberClan's Cybersecurity Maturity Model.

*Available at an additional cost



vCISO Advisory Services

CyberClan provides executive vCISO services for your organization, IT and Security teams Management, report and advising board of directors on all forms of Cyber Risk and plans to address them.

- Ongoing Governance Risk & Compliance Management
- Ongoing Risk Management
- Ongoing Compliance Management
- Ongoing Vendor Management Program
- Ongoing managing and directing IT and the security teams
- Ongoing engaging with executive management
- Ongoing running risk assessments on operational security
- Ongoing threat intelligence and managed enterprise security
- Criss Management

Information Security Policy Review/Development – How it Works

We request any policies you have

CyberClan reviews the documents against a benchmark and identifies gaps in existing policies or where policies should exist

CyberClan helps to build on what the organization already has or builds a custom policy from templates based on what the organization needs

The benefits of a vCISO service

- Hands-on assistance with a C-level expert
- C-suite board training on cyber resiliency
- Board of Directors presentation with information security best practices
- One-on-one sessions providing detailed feedback and guidance
- Continuous external validation
- Reduce cost in training



Simulated Phishing Campaign

Managed by the Insured

Powered by Wizer and with a focus on the hottest cybersecurity topics around, our training videos are created with the user in mind. We believe that to change behavior, security training should be personal; so, we took a personal approach.

By using conversational language, like "Scams" instead of "Data Breach" we made it relatable so that even Nana would get it.

We cut out all the BS and made all our videos 1-minute long and "to the point." That's probably why we have been rapidly growing with over 4000 organizations who have signed up for our training, whoa!

The training is offered in both English and French

*Available at an additional cost

SECURITY AWARENESS

- Wizer Intro
- Security Awareness Overview

COMMON THREATS

- Staying Safe of Public WIFI
- USB Safety
- Social Media Security
- Shadow IT – The Hidden Dangers

MOBILE SECURITY

- Mobile Security Threats
- Preventing Mobile Security Threats

PASSWORDS

- Creating a Strong Password
- 2FA
- Have I Been Hacked

PHISHING

- Phishing Overview
- Common Phishing Examples
- Detecting a Phishing Email
- What is BEC?
- Avoiding BEC Attack?
- What is Vishing?
- What is Smishing? RANSOMWARE
- What is Ransomware?
- Avoiding Ransomware

WORK FROM HOME

- Mindset
- Technology

BACK TO SCHOOL

- Mindset
- Technology





Simulated Phishing Campaign

Managed by the CyberClan

The CyberClan Managed Security Awareness Training (MSAT) Program is an off-the-shelf solution to comprehensive security awareness training. Developed by CyberClan's Risk Management Services Team of experienced security education professionals, it will help your organization achieve program success and phish rates as low as just 1%.

The training is offered in both English and French

*Available at an additional cost

MSAT Methodology

CyberClan takes a regularly updated and tested approach to workforce awareness, training, and education which can be customized to meet your organization's needs and culture and cover the most pertinent risks along with how to address them.

1. Evaluate
2. Train and Educate
3. Fortify
4. Measure and Repeat

Benefits of the MSAT Service

- Increased workforce awareness on cybersecurity, including how to avoid phishing and other types of social engineering cyberattacks
- An educated workforce can recognize potential malware behaviors and how to report possible security threats.
- Tailored curriculum to fit your organization
- Adherence to IT policies, best practices, and any applicable data privacy and compliance regulations is reinforced
- Additional internal communications resources provided through the program can enhance use knowledge retention
- Communication plans, templates and progress monitoring all in one place.

Managed Security Awareness Training Program Plans

Our program is designed to increase your workforce's awareness of cybersecurity, including how to avoid phishing and other social engineering cyberattacks. With an educated workforce, you can reduce the risk of potential malware behaviors and ensure that possible security threats are reported promptly. The program can be rolled out into one of three available tiers that covers a variety of training material and modules over the course of 12 months.



Tabletop Exercise

with Incident Response Workshop

*Available at an additional cost

Cyber breach response plans are paramount to reduce mistakes and chaos in a crisis and they work to mitigate business interruption while incident response and remediation take place. In a professionally guided, highly interactive, simulated scenario, key personnel and executives are asked to respond as they would.

Actions are then reviewed, assessed for improvements, and a plan is crafted to be distributed internally. As the regulatory environment continues to evolve and threat actors find new ways to breach a network, it's important that tabletop exercises are repeated for updates and inclusion of any new personnel.

Benefits of a CyberClan Tabletop Exercise

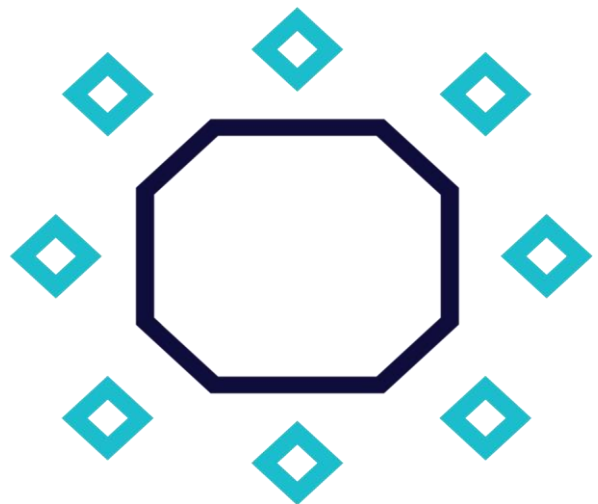
- Determines if emergency response actions are documented, understood, and accurate through informal discussion-based sessions, where team members discuss their roles and their responses to a particular emergency situation
- Helping leadership improve awareness, tabletop exercises work in conjunction with IR plans
- Learn Ransomware and Business Email Compromise best practices

How it Works

We request to see the plan document in scope for the Tabletop Exercise (i.e., the IR, DR, or BC Plan)

We develop a scenario based on the document and possible threats to the environment

We set up a discussion-based virtual meeting to run through the scenario with key stakeholders and staff





Business Continuity Planning Workshop

By CyberClan

*Available at an additional cost

Planning documentation are some of the most critical documents a company can maintain. If business functions experience downtime, or an incident causes damage to systems, the company should have plans documented, practiced, and ready in the event such situations.

CyberClan helps organizations tailor emergency plans to their business needs and prepare for real-world probable scenarios so they can continue operations.

Benefits of a Business Continuity Planning Workshop



- Help IT staff detect, respond to, and recover from network security incidents
- Help assess the level of detail documented in the organization's current plans and validate key measures they may take in the event of a crippling cyber-attack
- Can be combined with a tabletop exercise
- Provides detailed steps to maintain business operations if critical services are affected
- Allows for the availability of information and key staff in the event of an incident or disaster
- Enhances safety and decreases the potential for harm during an event

How it Works

We request any documentation that may exist in terms of Incident Response, Data Recovery, and Business Continuity Planning

We review the documentation and develop plans accordingly

CyberClan will send a questionnaire and/ or hold interviews with staff to identify process



Ransomware Readiness Assessment

Gap Assessments by CyberClan

*Available at an additional cost

A Gap Assessment provides a standardized method of assessing your current cybersecurity posture against future goals and objectives. Typically, this is based on using industry legal, regulatory and compliance national and international standards to improve your organization's performance.

With CyberClan's gap assessment, you get the expertise of an independent assessor to take a closer look at your existing policies, processes and procedures. The results are benchmarked against the requirements of the standard you want to achieve. Industry-standard examples are and are not limited to: ISO, NIST, CIS, PCI-DSS, HIPAA, SOC2, CMMC, Cybersecurity Essentials and many others.

The assessment results give your organization a view of any potential oversights or weaknesses so that you can take the appropriate action. It's also an excellent introduction to more formal auditing and gives your internal business functions teams the opportunity to understand what a certification audit will entail.

Benefits of a Gap Assessment

- Identify opportunities to improve your cybersecurity management processes, so you can take the right action to drive performance
- Give your stakeholders confidence in your organization's readiness to attain the standard and achieve certification
- Clarify the effort needed to achieve your desired standard using our independent observations, so you can plan resources, brief your team and get it right the first time.

How it Works

The gap assessment can be undertaken remotely or at your chosen location – remote assessments can provide greater flexibility, particularly if you want to move quickly

We'll review your processes and information to identify potential gaps against the requirements of your chosen standard

You'll receive a detailed written report so you know what actions to take to get closer to your goal

CyberClan offers assessments based on the following frameworks:

- NIST-Based Assessment
- CIS Assessment
- CMMC Level 1 Assessment
- HIPAA Assessment
- Business Impact Analysis
- Lightweight Risk Assessment

24/7 Managed Detection and Response Program with Security Warranty



*Available at an additional cost



The advantage cyber attackers have, is that they only have to be correct once to get it right. With CyberClan's managed detection and response program in your corner, you can be assured that you can outmaneuver even the most sophisticated attackers.



CyberClan is armed with unique intelligence and a complete picture of your attack surface, our Elite Threat Hunters and 24/7 Security Operations, and Incident Response Team are fully dedicated to protecting your business and containing threats with the potential to disrupt your business.

What you Can Expect from CyberClan's Managed Extended Detection and Response Program

- Six (6) months of Managed Detection and Response
- This program covers up to 150 endpoints, servers & cloud workloads
- Best-In-Class EDR Platform and enterprise-grade EDR included
- Average time to Contain: 15 minutes
- Our Security Program is designed on the NIST Incident Response Security Framework
- 24/7 Always on Monitoring
- 24/7 Live SOC Cyber Analyst Support
- 24/7 Threat Disruption and Containment & Remediation
- Machine Learning XDR Cloud Platform
- Automated Detection with Signatures, IOC and IP's
- Detection mapped to MITRE ATT&CK Framework
- Static and behavioral detection to neutralize known and unknown threats
- Detailed escalations with analysis and security recommendations
- Business Review and continuous improvement
- Suite features also include network control, USB and Bluetooth device control.
- Native network attack surface protection and rogue device identification available
- Security Warranty can provide up to \$2 million in coverage for forensic expenses, depending on the services provided, in the event of a network breach that is fully managed by CyberClan.



CyberClan's Security Operations are available 24/7 to address your questions or security events. Plus, when CyberClan calls, you know we are already engaged, initiating expert level incident response and containment as an extension of your internal team.



We balance each SOC rotation with mature technical and certified experts who proactively threat hunt, and we can contain threats in near real-time in your environment.

How we help put your business ahead of disruption:

- We provide security experts, cutting edge machine learning XDR technology and special intelligence from our incident response team members.
- Our SOC will keep watch around the clock to detect and mitigate threats in near real time.
- We take real ownership over protecting your business.



Additional Services

Clients who access these exclusive CyberClan risk management services are also eligible to access the following specialized services.*

*Available at an additional cost

Access to the CyberClan team 24/7/365

- 15-minute response from a dedicated hotline number and email address

CyberClan Perimeter Security Scorecard

- A point-in-time summary report of the client perimeter security scorecard
- The report includes the company's overall risk rate and a risk rate score for the below factors
 - Network Security
 - DNS Health
 - Patching Cadence
 - Endpoint Security
 - IP Reputation
 - Application Security
 - Cubit Score
 - Hacker Chatter
 - Information Leak
 - Social Engineering
- Semi annual scorecard baseline review with DUAL

CyberClan Incident Response Retainer

- A strategic, effective, and proactive risk management product that gives targeted coverage in the event of a network attack and/or breaches.

Continuous Vulnerability Management

- Our vulnerability assessment services help to identify and quantify internal and external weaknesses in a system.
- Utilizing best-in-class scanning tools and questionnaires to identify and grade vulnerabilities, we prioritize remediation, and create baselines for future comparisons.

CANADA

170-422 Richards
Street Vancouver BC
V6B 2Z4 Canada

UNITED STATES




1810 E Sahara Ave Las
Vegas NV 89104 USA

UNITED KINGDOM

Third Floor 43-45
Eastcheap London
EC3M 1JA UK

General Enquiries
US/CAD: 1855 685 5785
UK: 0800 048 7360
Email: info@cyberclan.com

24/7 Incident Hotline:
US/CAD: 1800 762 3290
UK: 0800 368 8731
We are open 24/7/365

 @cyber-clan
 @CyberClanTM
 @CyberClanOfficial