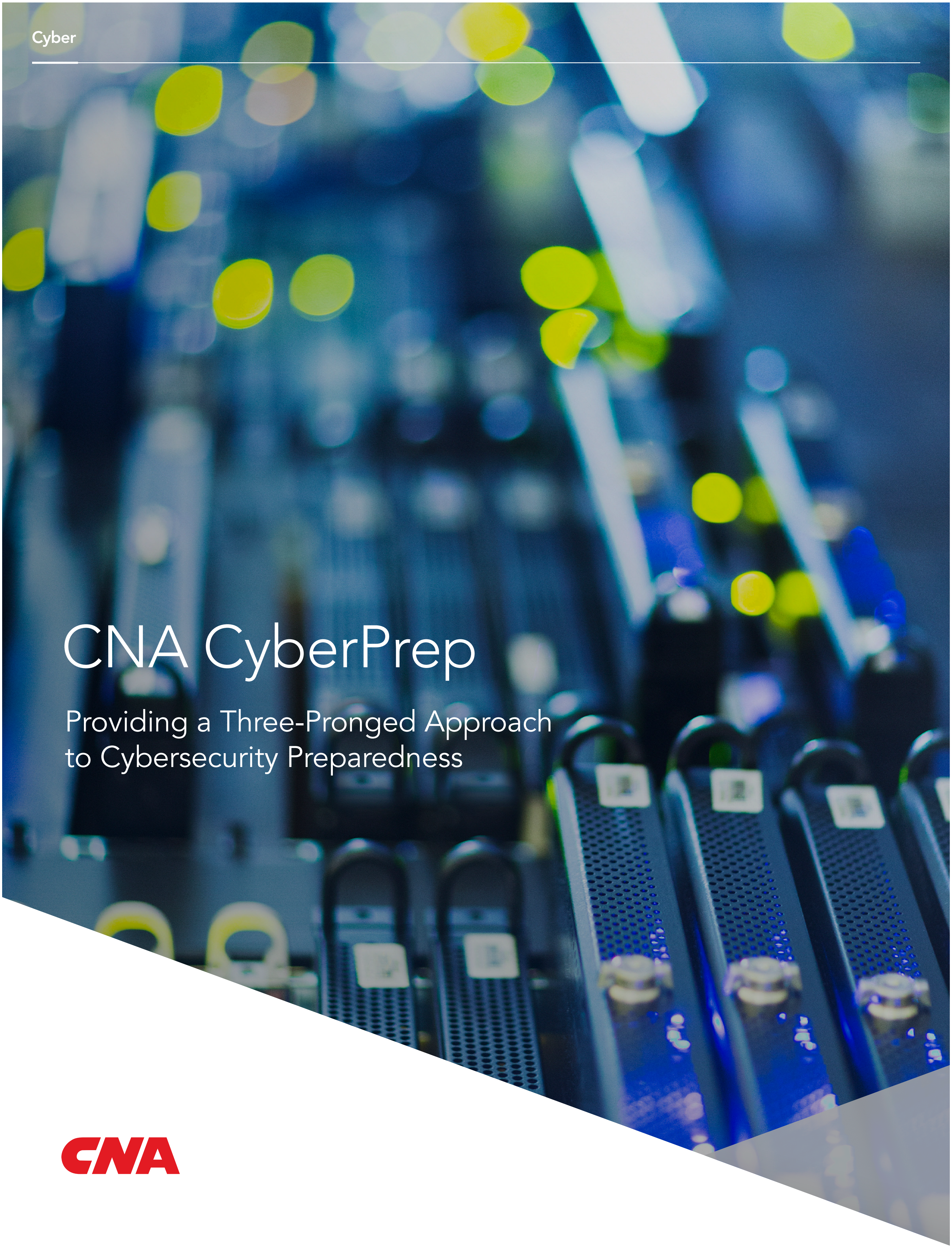


CNA CyberPrep

Providing a Three-Pronged Approach to Cybersecurity Preparedness

Cybercrime continues unabated, growing in sophistication, frequency and severity. In fact, cyber risk is one of the top risk concerns of companies globally according to World Economic Forum Global Risks Report 2021. CNA CyberPrep, built on nearly two decades of cyber insurance expertise, is a proactive program of cyber risk services developed by CNA Risk Control and CNA Cyber insurance underwriters in partnership with leading cybersecurity specialists. It is designed to aid CNA cyber policyholders in cyber threat identification, mitigation and response.

About CNA CyberPrep

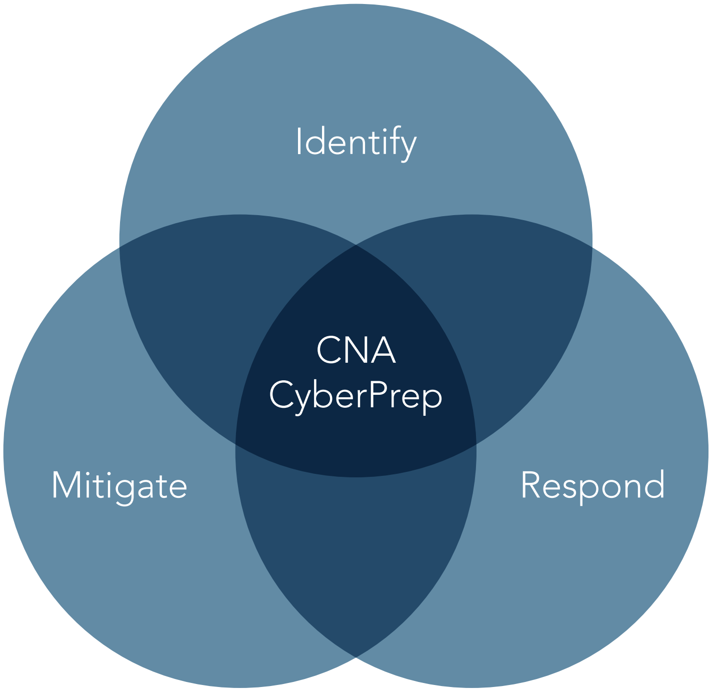
This brochure provides insureds with introductory information regarding these vendors and services. Insureds interested in more detailed information or to determine what services may be appropriate for their business, should contact their broker and CNA cyber underwriter.

Any reports and or recommendations provided by the vendors in the CyberPrep program (other than services provided by CNA Risk Control) will not be shared with CNA unless the insured and their broker choose to do so.

Use of the term "partnership" and/or "partner" should not be construed to represent a legally binding partnership.

CNA CyberPrep

CNA CyberPrep is available to all CNA cyber policyholders, providing them with a network of cybersecurity professionals and services to actively identify, mitigate and respond to their cyber risks. CNA CyberPrep is modeled on industry-leading cybersecurity frameworks for standards, guidelines and best practices, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and is rooted in strong partnerships with highly regarded cybersecurity professionals.



Identify

Identify current cybersecurity posture: A select group of vendors and services help insureds identify the strengths and weaknesses of their cybersecurity posture, while also providing recommendations for further cybersecurity steps.

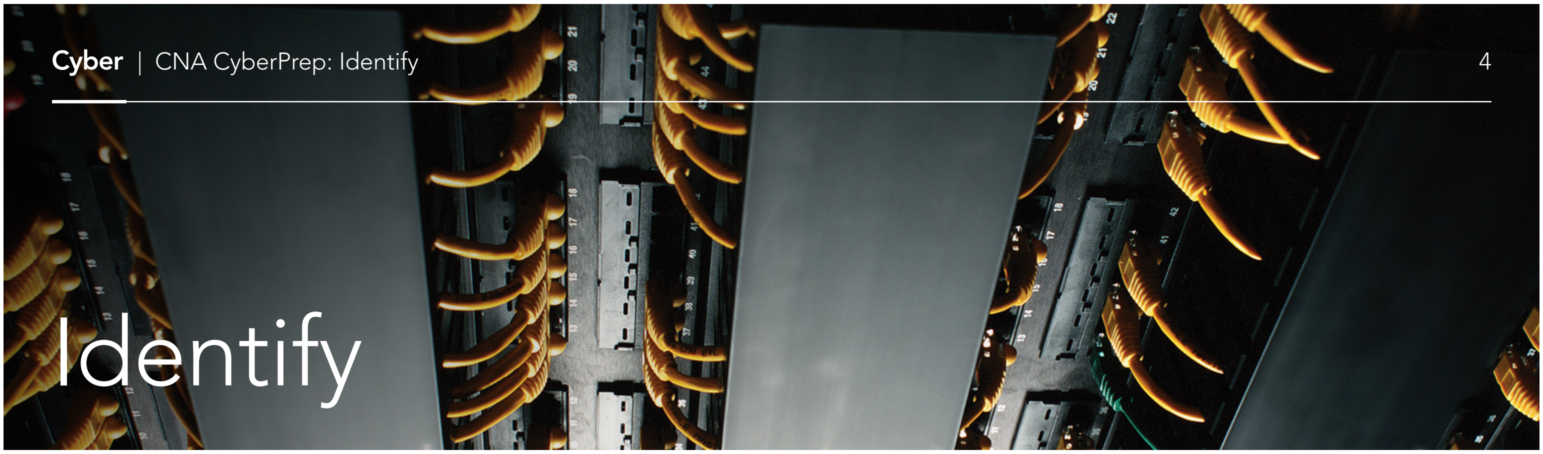
Mitigate

Mitigate potential cybersecurity risk: Cybersecurity recommendations are put into action by additional vendors and services, which help insureds enhance their cybersecurity posture by mitigating potential cyber risk. Services include next generation anti-virus protection, incident response planning and testing, policy and procedure development and testing, password management, employee education and multi-factor authentication.

Respond

Respond to cyber incident: Security incidents are often high-pressure situations. CNA's incident response vendors have a deep understanding of critical steps to minimize an incident's impact and provide help after one occurs. These vendors include breach/privacy counsel, forensic investigation and remediation firms, notification vendors, credit monitoring vendors and public relation firms.

Insureds are encouraged to speak with their broker and CNA cyber underwriter for more details on each service in this brochure.



Identify

Identifying cybersecurity posture is a critical beginning in the CNA CyberPrep process. Services include detailed analyses from a network of cybersecurity experts, reports that provide a snapshot of policyholder security posture and numerous recommendations for improvement. CNA cyber insureds may choose from fee-based preferred pricing services and value-added options, which are included as part of their CNA cyber policy.

Value-Added Services

CNA Risk Control Gap Analysis

The Gap Analysis analyzes information insureds provide about their existing information security programs. CNA offers a customized assessment designed to maximize information confidentiality and minimize vulnerabilities that may lead to a cyberattack.

The CNA Risk Control Gap Analysis:

- Scores the controls against common industry best practices
- Provides an estimated range of breach costs
- Identifies expected impact of loss prevention and mitigation efforts
- Provides recommendations that could potentially lower frequency and/or severity of loss for exposures identified as high impact

CNA Risk Control Information Security and Cyber Infrastructure Self-Assessment

This assessment tool is based on the principles of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover) and the NIST guidelines for Small Business Information Security. The results of the assessment help identify security control gap areas and create a baseline to address the potential impact of loss prevention and mitigation efforts.

GamaSec

GamaSec is a cybersecurity company that lowers the risk and strengthens the resilience of businesses from attacks on their websites and web applications. GamaSec provides a portfolio of services including web vulnerability scanning, daily malware detection, blacklist monitoring and application Firewall (WAF) with DDoS detection. This combination of a proprietary security platform and industry know-how enables GamaSec to deliver industry-leading solutions for website security.

Both existing and new qualifying policyholders in Canada have access to GamaSec. Using cutting-edge virtual hacker technology to identify and eradicate dangerous malware threats and website application vulnerabilities, GamaSec is a pre-breach tool designed to limit the impact of cyberattacks. It is easy to use and does not require coding or installation of additional software.

Value-Added Services

CyberArk – Privileged Access Security Assessment

CyberArk's Privileged Access Security Assessment systematically addresses organizations' privileged access security risk and recommends actions yielding the greatest improvement in their overall privileged access security posture. Evaluations are based on seven critical areas such as protecting against irreversible network takeover accounts and securing application credentials. A customized risk score enables the organization to benchmark its privileged access security maturity against peers using a reference group defined by industry, employee count, annual revenue and region. This detailed comparative analysis also provides remediation guidance.

After completing the assessment, the insured will receive a detailed report with the results and recommendations. A CyberArk representative is also available to discuss the report with the insured. *CNA will not receive the CyberArk assessment report unless the insured chooses to share it.*

Preferred Pricing Services

External Vulnerability Assessments

An external vulnerability assessment is an outside-in view of a network and/or website that seeks and identifies potential vulnerabilities, and recommends actions to help shore them up. The CNA CyberPrep network includes vendors that can provide insureds with external vulnerability assessments.

Penetration Testing

A penetration test is a simulated attack on your network and applications to determine and attempt to exploit vulnerabilities. At the conclusion of the test, a report will be provided with recommended steps to remediate identified vulnerabilities. The CNA CyberPrep network includes several penetration testing vendors that insureds may use.

Risk Assessments

CNA has established relationships with several vendors that offer risk assessments of varying types that help identify vulnerabilities in a business' cyber/IT environment.

Insureds are encouraged to speak with their broker and CNA cyber underwriter for more details on each service in this brochure.

Mitigate

Working in collaboration with their broker, CNA Risk Control and Cyber Underwriting, policyholders execute recommendations to **mitigate** their cyber risks and improve their cybersecurity posture. Recommendations may include using the following vendors, on either a fee-based preferred pricing service, or via value-added options included as part of their CNA cyber policy.

Value-Added Services

CNA's eRiskHub® Web Portal

CNA offers cyber policyholders access to eRiskHub®, an internet-based service that provides tools and resources to help clients understand the exposures, respond effectively and minimize the effects of breaches on their organizations. From prevention tips to response recommendations, eRiskHub® will assist with any cyber situation.

The eRiskHub® portal provides current cyber risk information and other powerful features, including:

- Incident Roadmap
- News Center
- Learning Center
- Risk Manager Tools
- eRisk Resources

Computer-Based Training Modules

CNA, through its relationship with Cofense, has the ability to provide cyber insureds with more than 20 cyber-related computer-based training modules, covering topics that include social engineering, phishing, breach response and other relevant topics. Please note: Computer based modules require a Learning Management System (LMS). Contact your broker or Cyber Underwriter to learn more about these services and purchasing a LMS at a preferred price if necessary.

CNA-Approved Breach Counsel Consultation

Each member of CNA's pre-approved breach counsel panel has agreed to provide CNA cyber insureds with a free one-hour consultation regarding the breach response process.

Ransomware Consultation

MoxFive, a leading incident management and technical advisory firm, will provide CNA cyber insureds with a free one hour consultation regarding the life cycle of a ransomware event, from prevention through response and remediation. With a focus on preventative assistance, MoxFive will discuss best practices regarding how to best prevent and respond to ransomware attacks, as well as best practices for implementing resilient backups and disaster recovery solutions.

Preferred Pricing Services

Ransomware Mitigation

MoxFive offers a full suite of services designed for ransomware preparation, mitigation and response. MoxFive works with organizations to advise on industry best practices and implement resilient backup and disaster recovery strategies and solutions that meet the demands of today's business and security requirements.

Incident Response Planning

Incident response planning is essential to an organization's cybersecurity platform. In fact, the first question a regulator often asks after an incident is reported is whether or not the company had an incident response plan (IRP). CNA has partnered with numerous vendors to provide essential incident response planning at preferred prices.

NetDiligence® Breach Plan Connect

Breach Plan Connect®, powered by NetDiligence®, helps insureds develop an IRP so they can respond efficiently and effectively when a breach event occurs. The software includes a pre-loaded comprehensive and actionable breach response plan. The "Build Your Plan" tool easily adapts the default plan for an insured's organization. The software includes an incident tracking report, incident response checklist and free cyber risk assessment survey.

Key Features

- Mobile-Friendly Platform – Access an IRP at any time, from anywhere, on any device
- Hosted Service – Access an IRP even when an organization's systems are compromised or inoperable
- Scheduled Reminders – Receive reminder emails to review and test an IRP
- Free Cyber Risk Assessment Survey – Evaluate and benchmark privacy and security practices

Breach Counsel: Each of CNA's pre-approved breach counsel panel is able to assist an insured with the creation, review, updating or editing of IRPs. Several of these firms have specific IRP services available at a preferred fixed rate for CNA cyber insureds.

Forensic Vendors: In addition to the options above, several of CNA's pre-approved forensic firms provide IRP services at a preferred fixed rate for CNA cyber insureds.

Policies and Procedures Development and Review

The development of cybersecurity and privacy policies and procedures is essential to an organization's cybersecurity platform. In fact, the second question regulators will ask after inquiring about an IRP is often whether the company has proper cybersecurity and privacy policies/procedures in place. The regulators will also want to review the policies and procedures.

Breach Counsel: Each member of CNA's pre-approved breach counsel panel is able to assist an insured with the creation, review, updating or editing of cybersecurity and privacy policies and procedures. Several of these firms have specific policy and procedure services available at a preferred fixed rate for CNA cyber insureds.

Forensic Vendors: In addition to the options above, several of CNA's pre-approved forensic firms can also review and prepare cybersecurity and privacy policies and procedures at a preferred fixed rate for CNA cyber insureds.

Tabletop Simulations

Once proper IRPs, policies and procedures are developed, it is critical that they are properly tested. CNA CyberPrep vendors are available to run simulations of various breach and attack scenarios to test the efficacy of a business' incident response, disaster recovery and business continuity plans, and also test whether policies and procedures respond properly to real world applications.

There are different kinds of tabletop simulations – some include a law firm, or a forensic firm, while others may include both. Pricing and scope may differ with each option.

Breach Counsel: Each of CNA's pre-approved breach counsel panel is able to assist an insured with tabletop exercises. Several of these firms have specific tabletop options available at a preferred fixed rate for CNA cyber insureds.

Forensic Vendors: In addition to the options above, all of CNA's pre-approved forensic firms can also provide tabletop options at a preferred fixed rate for CNA cyber insureds.

Insureds are encouraged to speak with their broker and CNA cyber underwriter for more details on each service in this brochure.

Preferred Pricing Services (cont'd)

CyberArk Red Team Tactics, Techniques and Procedures (TTP)

An engagement with the CyberArk Red Team will educate organization's Security Operations Team on the common attacks utilized by attackers to compromise security controls and put companies at significant risk. Security teams will receive the hands-on experience they need to understand popular attack techniques and defense strategies.

Security Awareness Training

Human error continues to be one of the top causes of cyber incidents. As a result, educating and training employees is a critical part of a robust cybersecurity platform. CNA has partnered with Cofense to provide security awareness and phishing campaign training to CNA cyber insureds.

Next Generation Anti-Virus Protection

Crowdstrike's Falcon Prevent is a unique array of powerful methods to prevent or protect against the rapidly changing tactics, techniques and procedures (TTPs) used by adversaries to breach organizations – including commodity malware, zero-day malware and even advanced malware-free attacks.

Password Management

Proper password management can help prevent many breaches, and is therefore a key control to have in place. CNA has partnered with Dashlane, a leading password management vendor, to offer a best-in-class password management product at a preferred price to CNA insureds.

Multi-Factor Authentication

Multi-factor authentication (MFA) is a redundant identification process, which requires users to utilize multiple verification steps to gain access to a network or system. The authentication process can entail a combination of passwords, texts, biometrics or other verification methods. The benefit of MFA: The more layers of security cyber criminals need to breach to gain access to a system, the more unlikely they are to try. CNA has partnered with Okta and WatchGuard to provide differing MFA offerings.

CyberArk Privileged Access Management Products

In addition to the Privileged Access Security Assessment outlined in the Identify section, CNA cyber insureds will have access to CyberArk's Privileged Access products, including:

Discover and Audit (DNA Workshop): A review of organizational requirements and drivers to identify objectives, success criteria, priorities and use cases of a privileged access security solution. With CyberArk, customers will conduct an in-depth review of critical controls and timelines using recommended CyberArk frameworks and tools such as CyberArk Privileged Access Security Cyber Hygiene Program and the Discovery and Audit (DNA) tool.

CyberArk Program Development Workshop: CyberArk industry-leading advisors help plan and develop a privilege access security program. This package accelerates the formulation of a privilege access security plan, saving time and money while slashing the development cycle from months to weeks.

Secure Your Endpoints and Plan Your Least Privilege Strategy

Privilege escalation is at the heart of most cyber attacks and system vulnerabilities. And yet, such security breaches often can easily be avoided by implementing the principle of least privilege, which is a pillar of zero-trust enterprise architectures. It applies to server environments, user workstations and control consoles for connected objects and machines in industry 4.0 factories to implement security by design. WALLIX offers an innovative, application-level security solution named BestSafe that enables organizations to completely eliminate administrator accounts, significantly reducing security incidents without impacting productivity and making it easier to comply with regulatory guidelines. Furthermore, if BestSafe is associated with the Bastion product line (PAM), it helps to elevate privilege when needed at the application level and not at the user level, preserving zero-trust architecture.

Insureds are encouraged to speak with their broker and CNA cyber underwriter for more details on each service in this brochure.

Respond

CNA CyberPrep continues to benefit policyholders over time. In the event of a cyber breach, CNA's panel of proven **incident response** vendors provide guidance and strategies to help expedite recovery and minimize loss in the event of a breach. Response services include breach counsel, forensic experts, notification and credit monitoring services and public relations.

Breach Counsel: CNA's approved breach counsel can help determine if confidential information was accessed and various provincial or territorial laws were triggered requiring a customer notification as the result of a data breach. Breach counsel can also help in interpreting the various regulations, insured's responsibilities under the law (if any), and assisting in crafting the customer notice letter.

Forensic Experts: CNA's approved forensic experts assist with post-breach investigation and remediation, such as determining the facts around the data breach incident and understanding the extent of the event.

Notification and Credit Monitoring Services: CNA's approved vendors provide insureds' customers with post-breach credit monitoring services.

Public Relations: CNA's approved public relations vendors assist with an insured's post-breach public communications efforts and potential publicity.

Insureds should reference the CNA Breach Incident Support overview or the post-breach tab on the eRiskHub® web portal for more information on these firms and services.

Insureds are encouraged to speak with their broker and CNA cyber underwriter for more details on each service in this brochure.

Cyber Privacy Event Support

Covering You Online, Offline, and Anywhere in the World

CNA has identified a network of proven breach coaches, forensics firms, and notification/call center vendors to assist in a timely and appropriate response to any privacy event. CNA understands that every situation is unique, and CNA's Claims team will work with you to choose the vendors that best fit your particular needs.

CNA Privacy Event Preferred Providers:

Pre-Breach Service

GamaSec
Avi Bar-Tov
gamasec.com
Email: a.bartov@gamasec.com
Mobile: + 972 54-4541718
US toll free 1 877 776 3925

Breach Counsel

Norton Rose Fulbright Canada LLP
Imran Ahmad, 416-863-4329, imran.ahmad@nortonrosefulbright.com
24/7 Email: nrfc.breach@nortonrosefulbright.com
24/7 Tel: 1-866-BREACHX / 1-866-273-2249

Fasken Martineau LLP
Alex Cameron, 416-865-4505, acameron@fasken.com
24/7 Email: acameron@fasken.com
24/7 Tel: 1-844-200-7505

Bennett Jones LLP
Ruth Promislow, 416-777-4688, promislowr@bennettjones.com
24/7 Email: bjresponse@bennettjones.com
24/7 Tel: 416-777-5500

Forensic

Arete Incident Response
1-866-210-0955
arete911@areteir.com

Charles River Associates
Aniket Bhardwaj
416-323-5574
abhardwaj@crai.com

CrowdStrike
Mike Vamvakaris
1-855-692-2052
mike.vamvakaris@crowdstrike.com
services@crowdstrike.com

Kivu Consulting, Inc.
1-855-548-8767
incidentresponse@kivuconsulting.com

Notification and Credit Monitoring

AllClear

Epiq Systems
416-603-3003

Equifax

Experian

Public Relations

FleishmanHillard HighRoad
fhhighroad.com
Phone +1-416-214-0701

CNA Risk Control Gap Analysis and Information Security and Cyber Infrastructure Self-Assessment Disclaimer

These tools are provided by CNA Risk Control to insureds to use as a reference for organizations seeking to evaluate risk exposures associated with their current Information Security Policies, Procedures and Controls. The content produced is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. CNA Risk Control does not implement any security controls nor develop policies or procedures for the Insured. Information Security Policies, Procedures and Controls should be developed by each Insured and tailored to the Insured's individual security profile. These statements do not constitute a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice, including advice of legal counsel, given after a thorough examination of the individual situation, encompassing a review of relevant facts, laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

The goal of CNA CyberPrep's Identify stage is to help an insured better understand its Information Security Posture while possibly identifying potential threats and vulnerability areas. Ideally, the answers obtained in the Identify stage will help you prioritize your risk mitigation efforts. Make sure you include key stakeholders in the self-assessment process. The self-assessment should be repeated at least annually and when business conditions change.

About CNA

CNA is one of the largest U.S. commercial property and casualty insurance companies. Backed by more than 125 years of experience, CNA provides a broad range of standard and specialized insurance products and services for businesses and professionals in the U.S., Canada and Europe.

For more information, please visit cnacanada.ca.

CNA