Cyber & Professional Lines Group
16501 Ventura Blvd. Suite 200, Encino, CA 91436
main (818) 382-2030

TechGuard® Cyber Liability Insurance Renewal Application

THIS IS AN APPLICATION FOR A CLAIMS MADE AND REPORTED POLICY. THIS APPLICATION IS NOT A BINDER.

This application for TechGuard® Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant.

1. GENERAL INFORMATION			
Name of Applicant			
Street Address		Phone	
City, State, Zip		Fax	
Website		Contact e-mail	
Applicant is a(an): ☐ Individual ☐ Corporation ☐ Partnership ☐ Other: _____			
Square footage for all locations owned or leased by the Applicant (**If applying for General Liability Insurance**)			

2. REQUIRED ADDITIONAL INFORMATION	
a. Has the name of the Applicant changed, or has any merger or consolidation taken place, in the past 12 months? **If "Yes", please provide details on a separate page.**	☐ Yes ☐ No
b. Have there been any material changes in the Applicant's security controls in the past 12 months? **If "Yes", please provide details on a separate page.**	☐ Yes ☐ No
c. Has the Applicant acquired any subsidiaries, affiliated companies or entities in the past 12 months? **If "Yes", please attach a list with a description of (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant.**	☐ Yes ☐ No
d. Has the Applicant changed the nature of its professional services in the past 12 months? **If "Yes", please provide details on a separate page.**	☐ Yes ☐ No

3. REVENUES		
	Current Fiscal Year ending / (current projected)	**Last** Fiscal Year ending /
Total gross revenues:	$	$

4. RECORDS	
a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? **If "Yes" please provide the approximate number of unique records**: **Paper records:** _____ **Electronic records:** _____ ***Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.**	☐ Yes ☐ No

b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? **If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws?**	☐ Yes ☐ No ☐ Yes ☐ No
5. INFORMATION AND NETWORK SECURITY CONTROLS	
a. Do you use anti-virus software and a firewall to protect your network?	☐ Yes ☐ No
b. Do you use a cloud provider to store data? **If "Yes", please provide the name of the cloud provider:** _____ **If you use more than one cloud provider to store data, please specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.**	☐ Yes ☐ No
c. Do you encrypt all sensitive and confidential information stored on your organization's systems and networks? **If "No", are the following compensating controls in place:** **(1) Segregation of servers that store sensitive and confidential information?** **(2) Access control with role-based assignments?**	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
6. RANSOMWARE CONTROLS	
a. Do you use 2-factor authentication to secure remote access to your network?	☐ Yes ☐ No
b. Do you use 2-factor authentication to secure remote access to your email accounts?	☐ Yes ☐ No
c. Do you use Endpoint Detection and Response (EDR) or a Next-Generation Antivirus (NGAV) software (e.g., CrowdStrike, Cylance, Carbon Black) to secure all system endpoints? **If "Yes", please list your provider:** _____	☐ Yes ☐ No
d. Do you use an email filtering solution designed to prevent phishing or ransomware attacks (in addition to any filtering solution(s) provided by your email provider)? **If "Yes", please provide the name of your filtering solution provider:** _____	☐ Yes ☐ No
e. Do you use a data backup solution for all critical data? **If "Yes":** **(1) How frequently does it run?** ☐ **Daily** ☐ **Weekly** ☐ **Monthly** **(2) Which of the following best describes your data backup solution?** ☐ **Local backup** ☐ **Network drive** ☐ **Tape backup** ☐ **Off-site storage** ☐ **Cloud backup** ☐ **Other**: _____ **(3) Please list your data backup provider:** _____ **(4) Is your data backup solution segregated or disconnected from your network in such a way to reduce or eliminate the risk of the backup being compromised in a malware or ransomware attack that spreads throughout your network?**	☐ Yes ☐ No ☐ Yes ☐ No
7. PHISHING CONTROLS	
a. Do all employees with financial or accounting responsibilities at your company complete social engineering training? **If "Yes", does such training include phishing simulation?**	☐ Yes ☐ No ☐ Yes ☐ No

b. Does your organization send and/or receive wire transfers?	☐ Yes ☐ No
If "Yes", does your wire transfer authorization process include the following:	
(1) A wire request documentation form?	☐ Yes ☐ No
(2) A protocol for obtaining proper written authorization for wire transfers?	☐ Yes ☐ No
(3) A separation of authority protocol?	☐ Yes ☐ No
(4) A protocol for confirming all payment or funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the payment or funds transfer instruction/request was received?	☐ Yes ☐ No
(5) A protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the change request was received?	☐ Yes ☐ No

8. LOSS HISTORY

If the answer to any question in 8.a. through 8.c. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. In the past 12 months, has the Applicant or any other person or organization proposed for this insurance:	
(1) Received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the Applicant's network?	☐ Yes ☐ No
(2) Been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation?	☐ Yes ☐ No
(3) Notified customers, clients or any third party of any security breach or privacy breach?	☐ Yes ☐ No
(4) Received any cyber extortion demand or threat?	☐ Yes ☐ No
(5) Sustained any unscheduled network outage or interruption for any reason?	☐ Yes ☐ No
(6) Sustained any property damage or business interruption losses as a result of a cyber-attack?	☐ Yes ☐ No
(7) Sustained any losses due to wire transfer fraud, telecommunications fraud or phishing fraud?	☐ Yes ☐ No
b. In the past 12 months, has any IT service provider that the Applicant relies on sustained an unscheduled network outage or interruption lasting longer than 4 hours?	☐ Yes ☐ No
If "Yes", did the Applicant experience an interruption in business due to such outage or interruption?	☐ Yes ☐ No
c. In the past 12 months, has the Applicant or any other person or organization proposed for this insurance received any complaints or written demands or been a subject in litigation involving any wrongful act, error or omission in the performance of, or failure to perform, professional services?	☐ Yes ☐ No
d. Has the Applicant notified Tokio Marine HCC of all incidents or losses occurring, or claims, suits or demands received, in the past 12 months?	☐ Yes ☐ No
If "No", please forward complete details to Tokio Marine HCC immediately.	☐ None to Report

9. GENERAL LIABILITY LOSS HISTORY

Please answer questions 9.a. & 9.b. below only if General Liability Coverage is desired.

If the answer to question 9.a. or 9.b. below is "Yes", please complete a Claim Supplemental Form for each claim, allegation or incident.

a. In the past 12 months, did the Applicant or any other person or organization proposed for this insurance receive knowledge of any situation(s), circumstance(s) or allegation(s) of bodily injury, property damage, or personal and advertising injury, that may give rise to a claim?	☐ Yes ☐ No
b. In the past 12 months, has any claim for bodily injury, property damage or personal and advertising injury been made against the Applicant or any other person or organization proposed for this insurance?	☐ Yes ☐ No
c. Has the Applicant notified Tokio Marine HCC of all reports, allegations, claims, suits or demands involving or arising from bodily injury, property damage, or personal and advertising injury received in the past 12 months?	☐ Yes ☐ No
If "No", please forward complete details to Tokio Marine HCC immediately.	☐ None to Report

NOTICE TO APPLICANT

NOTICE TO NEW YORK APPLICANTS: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

The Applicant hereby acknowledges that he/she/it is aware that the limit of liability shall be reduced, and may be completely exhausted, by claim expenses and, in such event, the Insurer shall not be liable for claim expenses or any judgment or settlement that exceed the limit of liability.

I HEREBY DECLARE that, after inquiry, the above statements and particulars are true and I have not suppressed or misstated any material fact, and that I agree that this application shall be the basis of the contract with the Underwriters.

CERTIFICATION AND SIGNATURE

The Applicant has read the foregoing and understands that completion of this application does not bind the Underwriter or the Broker to provide coverage. It is agreed, however, that this application is complete and correct to the best of the Applicant's knowledge and belief, and that all particulars which may have a bearing upon acceptability as a TechGuard® Cyber Liability Insurance risk have been revealed.

It is understood that this application shall form the basis of the contract should the Underwriter approve coverage, and should the Applicant be satisfied with the Underwriter's quotation. It is further agreed that, if in the time between submission of this application and the requested date for coverage to be effective, the Applicant becomes aware of any information which would change the answers furnished in response to any question of this application, such information shall be revealed immediately in writing to the Underwriter.

This application shall be deemed attached to and form a part of the Policy should coverage be bound.

Must be signed by an officer of the company.

Print or Type Applicant's Name	Title of Applicant
Signature of Applicant	Date Signed by Applicant

TOKIO MARINE HCC

Email fraud can cost you millions.

1. Do you have dual-factor authentication implemented on all company email systems?
2. Are your employees regularly trained to recognize phishing emails?
3. Is your email configured to help identify suspicious behavior?

You can protect your business.

We can help.

What is Business Email Compromise (BEC)?

Business email compromise (BEC) or "phishing" is a technique used to gain access to your company email so criminals can impersonate a co-worker, manager or other trusted business partner to steal sensitive data and money.

With access to your business email accounts, criminals can steal money through fraudulent wire transfer requests, fake invoices, diverting payroll and more. Protecting your email is essential. BEC emails usually contain no malware and are therefore difficult to detect with common email filtering means.

How does a typical BEC scam work?

A common technique is email spoofing. Email spoofing occurs when the email appears to be sent by a legitimate sender but is actually sent by a criminal.

For example, your accounts payable department receives an email from the CEO (who is traveling abroad) asking for $100,000 to be immediately wired to a new bank account of a trusted business partner. The employee complies. You later discover the new bank account belongs to a criminal who spoofed the CEO's email account to divert the money. You immediately call the bank but the money has already been transferred.

Get your email systems cyber ready!

Contact our cyber experts at:
877.244.9688

Cyber criminals get your email credentials by tricking you.

Here's how the bad guys work:

Phishing pages: Bad guys send a link to a bogus login page for a false Office 365 or Google page requesting your credentials. The page looks identical to the real O365 or Google login page.

- **O365 example:** You get an email stating Jane Doe shared a file with you. When you click the link, it opens a fake O365 page and you enter credentials. Your credentials are now compromised.

- **Google example:** You get an email that appears to be from Google warning you that your account may have been compromised, and you need to change your password. The website will provide a link to a fake Google login page where you enter your credentials. Your credentials are now compromised.

Another common way to steal credentials is via "Keyloggers". A keylogger is malicious software that captures your keyboard strokes without you knowing.

A phishing email may contain an innocent-looking link, but when you click the link, a keylogger is instantly downloaded and installed. Now, all keystrokes (including your personal bank accounts, social media, etc.) are sent to bad guys, including your usernames and passwords..

Protect Yourself and Your Company

1. (2FA) – A dual authentication method that includes something you know (password) and something you have (e.g. text message to your phone or a confirmation within a smartphone app).

2. Phishing Training – Online or in-person training and simulation.

3. Spam Filtering & Email Configuration

How to prevent BEC attacks

Three easy steps can save your business.

1. Enable Dual-Factor Authentication (2FA) on Email

We **strongly** recommend you implement this simple and cost-effective measure.

This is the easiest and most effective thing your organization can do to reduce the risk of transfer fraud and it doesn't cost a thing!

2FA protects your organization because it adds another layer of protection to password-protected remote access to your network. In other words, even if the hacker has stolen an employee's login credentials, dual-factor authentication should prevent them from accessing your email and network, since they would also need to have the employee's mobile phone which is being used as the 2nd authentication factor.

Information on how to enable 2FA on O365 and GSuite can be found below:

Microsoft Office 2FA Support

Google 2FA Support

2. Employee Training to Recognize Phishing

Teaching your employees to stay alert and recognize dangerous phishing emails is a great way to thwart BEC attacks. Employees should never click on an attachment or link an email from an unverified sender. Training your employees will protect your company from the number one cause of a cyber attack—human error.

Helpful Tip!

Conducting a live phishing simulation is another great way to train employees to recognize dangerous BEC/phishing emails. Phishing simulations help identify those employees who are susceptible to phishing attacks and require additional training.

Your TMHCC cyber insurance policy gives you **free** access to phishing simulation services and numerous employee cybersecurity training courses. For more information on free employee training and phishing simulation services, contact ePlace Solutions.

3. Spam Filtering & Email Configuration

Your email server can automatically filter out certain suspicious phishing emails. Activating these filters is an easy way to prevent dangerous phishing emails from landing in your employees' mailboxes. Use email filtering to quarantine suspicious emails, and scan documents and files before they are opened.

In Office365, administrators can develop alert policies to detect specific behavior. To do so, log into protection.office.com, go to *Security and Compliance center > Alerts > Manage Advanced Alerts. Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both.*

It is also recommended to create a rule for "Set-InboxRule." Details can be found here: **https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies**

Email solutions which can help mitigate the risk of BEC include Proofpoint, Mimecast, and Ironscales.

Your Tokio Marine HCC cyber insurance policy includes cyber security services (like employee cyber security training and phishing simulation services) to protect your organization against costly cyber attacks. There's no cost to you.

To learn more about these free services, contact our partner ePlace Solutions at support@eplaceinc.com or 877-244-9688.

TOKIO MARINE HCC

TOKIO MARINE HCC

Don't Let Ransomware Destroy Your Business

Do you...

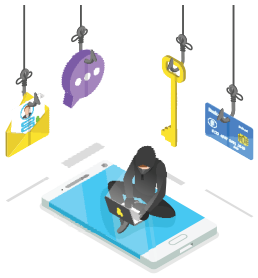
1. Require two-factor authentication for all remote access to your network?
2. Have a secure data backup solution in the event of a ransomware attack?
3. Use the right email spam filter?
4. Fight malware with behavior-based antivirus software?

You can protect yourself and your organization. And we can help.

There are 5 key cyber smart strategies:

1. Remote Desktop Protocol
2. Two-Factor Authentication
3. Offline Backups
4. Spam Filtering & Email Configuration
5. Next Generation Anti-Virus: Behavior-based Protection

RANSOM DEMANDS HAVE INCREASED 40x FROM 2016 TO 2019



Your Tokio Marine HCC cyber insurance policy offers free cyber security services (like employee cybersecurity training and phishing simulation services) to protect your organization against costly cyber attacks.

For more information on these services, contact our cyber security experts at ePlace Solutions at support@eplaceinc.com or 877-244-9688.

You Can Prevent Ransomware Attacks

Just a few easy steps can save your business. Call us to help guide you through 877.244.9688

1. Lockdown Remote Desktop Protocol Across Your Entire Organization

More than 60% of ransomware attacks originate from hackers gaining unauthorized access to a computer via Remote Desktop Protocol (RDP). Using compromised credentials, a hacker can login to a computer within your company's network using RDP, move within the network undetected, and launch a crippling ransomware attack on your organization. Login credentials are highly vulnerable to theft from social engineering techniques and assorted malware variants, so they cannot be solely relied upon to protect your organization. Compromised RDP credentials are available for sale on the dark web for as little as $3.

The easiest way to avoid having criminals get access to your network via this method is to simply disable this feature on all machines/servers on your network. If you absolutely need to use RDP, we recommend placing RDP access behind a VPN that is protected by multi-factor authentication, which add an important additional layer of security. Alternatively a Remote Desktop Gateway Server can be utilized, which can also be protected with multi-factor authentication.

A typical, real-life ransomware attack

Your employee receives an email seemingly from Microsoft, warning them that their account may have been compromised, and to login to verify that they are the owner of the account. The user inputs their login and password, and the credentials are stolen by a hacker using this rudimentary but highly successful phishing technique. The criminal notices that your employee's computer has the **Remote Desktop Protocol (RDP)** enabled, and logs into the employee's computer while they work from home, using the stolen credentials. The hacker uses the hijacked computer to find the backup server on the company's network, and deploys ransomware to encrypt the company's backups, before launching a wide-ranging attack on the rest of the company's computers and servers. This attack cost the company over $10,000,000 between the 7-figure ransom payment, related expenses and business interruption losses.

2. Two-Factor Authentication (2FA)

We strongly recommend you implement this simple and cost-effective security measure. 2FA protects your organization because it adds another layer of protection to password-protected remote access to your network. The vast majority of successful hacking/ransomware attacks are a result of the hacker gaining access to a company's network using compromised login credentials. In other words, even if the hacker has stolen an employee's login credentials, dual-factor authentication should

Continued on next page

You Can Prevent Ransomware Attacks

prevent them from accessing your network, since they would also need to have the employee's mobile phone which is being used as the 2nd authentication factor.

2FA should also be used on all remote access to your email servers (**Office 365** and **GSuite** have free solutions). Hackers use compromised email accounts to launch ransomware or social engineering attacks against your contacts.

3. Offline Segregated Backups

Backups can be another effective strategy to reduce ransomware damages and business disruption. If you get infected with a ransomware virus, you may not need to pay the ransom to get back up and running if you have an intact backup. You will be able to wipe out the virus, clean your devices and network, and reinstall everything from a recent, clean backup.

Recently hackers have been effectively attacking backups that are not properly protected. All backup solutions that are connected and mapped on your network are highly vulnerable to malware/hackers. Having a properly segregated backup is an effective technique to reduce this risk.

So consider the cloud. For small and medium sized companies, Veeam, Datto, Backblaze and iDrive provide popular cloud solutions for backups. Just because you are using the cloud does not mean the cloud backups are properly isolated or segregated. Be sure to properly configure any cloud backups to ensure they are isolated from your operating environment.

Create internal procedures for maintaining on-site and off-site backups of your critical systems and data. Best practices include periodically testing your backups by restoring your systems from backup to ensure they work when needed.

4. Spam Filtering & Email Configuration

Your email server can automatically filter out suspicious emails. Activating these filters is an easy way to prevent dangerous phishing emails from landing in your employees' mailboxes. Use email filtering to quarantine suspicious emails and scan documents and files before they are opened.

Because criminals are using a compromised account concurrently with the actual user, they must hide their activity. Check your email for suspicious email forwarding and mailbox rules. These rules are a signature that reliably detect whether criminals have infiltrated your email.

Call us for help with your cyber security plan 877.244.9688

Helpful Tip!

In Office365, administrators can develop alert policies to detect specific behavior. To do so, log into protection.office.com, go to **Security and Compliance center > Alerts > Manage Advanced Alerts. Create a new alert for "New-InboxRule Create Inbox rule from" and select Outlook or Outlook Web App or both.**

It is also recommended to create a rule for "Set-InboxRule." Details can be found here: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

5. Next Generation Anti-Virus: Behavior-based Protection

Behavior-based security software scans devices for unusual behavior and can decide if the deviation is a threat. These solutions are typically connected to the cloud, so their ability to detect new malware variants is updated in real time. This is sometimes known as Next Generation Anti-Virus.

Anti-virus software on user devices, networks and servers is used to find or block suspicious activity. Traditional anti-virus relies on a vast database of virus signatures to help the software identify malicious applications on your computers. Modern malware can easily be modified to not match existing signatures. Popular NGAV end point protection tools include Microsoft Defender Advanced Threat Protection, BitDefender Gravity Elite, CarbonBlack and CrowdStrike's Falcon/Protect. Behavior-based endpoint protection is an efficient way to protect against new threats and prevents ransomware from spreading throughout your network.

THE AVERAGE RANSOMWARE DEMAND INCREASED 7x YOY IN 2019

For more information about ransomware solutions and all of our cyber security services, contact our cyber experts at ePlace Solutions at support@eplaceinc.com or 877-244-9688.

Don't just be insured, be prepared.

TOKIO MARINE HCC