CHURCH INSURANCE COMPANIES
Insurance for the Greater Good

Risk Management Factsheet

Copyright: Risk Management Resources for Churches

What is copyright?

Copyright is a form of protection granted by law for original works of authorship fixed in a tangible medium of expression. Copyright can protect both published and unpublished works.

What does copyright protect?

Copyright, a form of intellectual property law, protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture.

What is copyright infringement?

According to the United States Copyright Office, if you reproduce, distribute, publicly perform, publicly display, or derive a new piece from a copyrighted work without the permission of the copyright owner, you may have infringed on copyright. That could include putting a poem or song on your website, printing an essay or column in your bulletin, or even streaming a service on your website that includes the performance of hymns from a hymnal you have purchased. The safest thing a church can do is only to use copyrighted materials when you have the express written permission of the copyright owner. This is generally accomplished by purchasing the appropriate license.

How do copyrights impact the Church?

To better understand the impact of copyright from a church perspective, let's look at the use of music as an example. A church is free to use any work no longer protected by copyright (public domain). An example of a Christmas song in the public domain is "Silent Night, Holy Night."

Additionally, the Religious Services Exemption (RSE) allows congregants to sing hymns during service without first getting permission. It also allows pastors to recite poems in their sermons. The RSE only applies while services are being conducted in-person at a religious gathering. The exemption excludes performance activities at a place of worship that are for social, educational, fund-raising, or entertainment purposes. *Lastly, the RSE does not allow for the printing and or streaming of material covered by copyright.*

Church Streaming and Internet Posting

The pandemic has seen a dramatic increase in the number of congregations streaming their services on line. Since the congregations are now technically broadcasting, extra care needs to be paid to ensure against copyright infringements; specifically but not limited to the use of protected music. A solution is for the church to obtain permission to use materials protected by copyright and this often involves paying a licensing fee.

Respecting Copyright Laws

Rectors and church leaders use a variety of methods to connect with their members. Sometimes a poem or a song might seem like just the thing; it might say something profound in a particularly lovely way. However, if you discover a piece you would like to share with the rest of the church population, you have to be careful that you're not infringing on a copyright.

FAQs

Q: How can our church obtain a license to print copies of lyrics and / or sheet music and perform (sing) them in the course of our church services

A: While it is important to remember that not all works protected by copyright are available for licensing. Your church must obtain the appropriate license from the copyright owner or a licensing organization that has the right to license the music you are interested in using. You will need to review your specific needs to find the appropriate licensing organization for your situation. While we don't endorse any particular organization, some include:

- **OneLicense.net** *onelicense.net* – is a service that licenses copyright permission to reprint, podcast, and record hymns and songs for your congregation from an impressive list of Member Publishers.
- **Christian Copyright Solutions** (CCS) *christiancopyrightsolutions.com* – partners with the Performing Rights Organizations to offer licenses to religious organizations covering over 29,000,000 Christian and secular songs.
- **RiteSong** *riteseries.org* – is an online music library owned by Church Publishing Incorporated (CPI) for hymns and other liturgical music. It includes permission to use all hymns available through the program for print congregational use. Subscriptions provide access to nearly 2,000 hymns from *The Hymnal 1982, The Hymnal 1982 Service Music, Wonder, Love and Praise, Lift Every Voice and Sing II, Enriching Our Music 1 & 2, Voices Found, and My Heart Sings Out*.
- **RitePlanning** *riteplanning.com* – is a customizable worship planning tool also owned by CPI with a comprehensive library of liturgical and music resources. A subscription to the deluxe version includes permission for hymns and other music to be reproduced for use in a bulletin or service leaflet.

Q: In addition to printing copies of lyrics and / or music and singing them in the course of our church services, how can our church obtain a license to stream our church services over the internet?

A: A church must obtain the appropriate license from a licensing organization for streaming and / or internet use. However, the church will want to be clear about the type of use (streaming / internet) they are seeking to license so that the licensing organization can provide them with the appropriate solution.

Q: Is our church able to play sound recordings of secular songs?

A: A church would need to acquire the appropriate licenses from the copyright owner to play sound recordings of secular songs.

Q: How do artists or publishers find out their material is being used without permission?

A: The internet makes it easy to discover if materials are being used without permission. For example, artists could set up alerts for certain phrases or names, which would inform them when the material gets posted on a website. Then, it is easy to check whether the individual who has posted the material obtained permission and paid a licensing fee (if required).

Q: What happens when artists or publishers finds an infringement of their copyright?

A: Typically, if you are caught infringing on copyright, the publisher sends a demand letter, asking that you immediately stop and perhaps a demand for a certain amount of money. If you need to take down infringing content, have your webmaster remove the materials from your website. If you just delete the text, it is possible that people searching the internet might see a cached image of your site, which would still contain the copyrighted material.

LIABILITY (THIRD PARTY) COVERAGE SUMMARY: COVERAGE FOR CLAIMS MADE AGAINST YOU

Multimedia Liability – Duty to defend coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.

Security and Privacy Liability – Duty to defend coverage for third party claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.

Privacy Regulatory Defense and Penalties - Duty to defend coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, or local governmental agencies, such as proceedings/investigations alleging HIPAA violations.

PCI DSS Liability - Duty to defend coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

NON-LIABILITY (FIRST PARTY) COVERAGE SUMMARY: COVERAGE FOR YOUR OWN LOSSES

Breach Event Costs –Reasonable and necessary mitigation costs and expenses incurred because of a privacy breach, security breach or adverse media report, including legal expenses, public relations expenses, advertising and IT forensic expenses, postage, and the cost to provide call centers, credit monitoring and identity theft assistance.

Proactive Privacy Breach Response Costs (sub-limit of Breach Event Costs) - Public relations expenses incurred in response to a security breach or privacy breach, but prior to the publication of an adverse media report, to avert or mitigate reputational harm which could result from the adverse media report.

Voluntary Customer Notification Expenses (sub-limit of Breach Event Costs) - Expenses incurred in notifying parties of a privacy breach where there is no requirement by law to do so.

BrandGuard® - Lost revenue incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

Network Asset Protection – Reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased or corrupted due to (1) accidental damage or destruction of electronic media or computer hardware, (2) administrative or operational mistakes in the handling of electronic data, or (3) computer crime/attacks including malicious code and denial of service attacks. Coverage also extends to business income loss and interruption expenses incurred because of a total or partial interruption of an insured computer system directly caused by any of the above events.

Cyber Extortion – Extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

Cyber Crime –Loss of money or securities incurred due to financial fraud, including wire transfer fraud; charges incurred for unauthorized calls resulting from fraudulent use of an insured telephone system; expenses incurred to notify customers of phishing schemes that impersonate the Insured or the Insured's brands, products or services, and the costs of reimbursing customers for losses resulting from such phishing schemes.

Cyber Loss Examples

1. Ransomware encrypted five workstations and one server. We assigned a breach attorney and retained Navigant to perform a forensic investigation. Counsel, through the investigation, determined that the notification would not be required under Ohio data breach laws.

2. Two computers were stolen from the Insured. We assigned a breach attorney, who determined that affected individuals had to be notified of the breach. We paid for credit monitoring for the affected individuals.

3. Insured reported suspected security breach. Former employees were suspected of gaining access to the system and deleting files. The Insured handled the matter internally and requested that we close the file.

4. Insured was tricked into wire transferring funds due to a spoofed email. We paid the crime loss.

5. The Insured's CFO received an email purporting to be the Insured's bishop requesting a wire transfer. The CFO authorized the payment but was able to stop the transfer upon discovering the fraud. We assigned a breach attorney to assess, in conjunction with the Insured's IT, whether a breach had occurred. The investigation reveal that no breach occurred.

6. Insured reported a ransomware event. However, insured was able to restore from a backup. Insured requested that file be closed.

7. Insured received a spoofed email and wire transferred approximately $62K to a malicious actor who purported to be the Insured's contractor. The Insured also suspected a security breach, so we assigned a breach attorney. We paid the $25K cybercrime limit and costs associated with investigating the breach.

8. Insured reported a ransomware event. However, Insured's IT vendor was able to restore from a backup. We paid IT expenses.

9. Payroll fraud. Insured was tricked into changing direct deposit information. We paid for the loss.

10. Employee's computer encrypted by a virus. Data was restored from a backup, but laptop contained PII for about 50 current and former employees. We paid notification costs.

11. Disgruntled former employee wiped information from the Insured's system. The Insured believes that PII has been accessed. We recently assigned a breach attorney to assist. We expected expenses shortly.

12. Covered Cyber Crime claim. Employee was tricked into buying gift cards by someone purporting to be another employee. However, $1000 loss fell within the retention.