Cyber Claim Prevention and Response

Jeff Koch, President & CEO
United Methodist Insurance

www.uminsure.org
Understanding Cybercrime

- **WHAT**: Criminal activities carried out using digital technology and the internet.
- **HOW**: Hacking, identity theft, data breaches, malware attacks, phishing, ransomware, and more.
- **WHY**: For financial gain, political motives, personal vendettas, or a combination thereof.
Potential Impact of Cybercrime

Potential Impact of Cybercrime

- Financial Loss
- Data Breaches
- Reputation Damage
- Operational Disruption

Preventive Measures
Preventive Measures

Education and Training
- Conduct cybersecurity awareness programs:
  - administrators
  - Staff
  - congregation members
- Know best practices:
  - creating strong passwords
  - recognizing phishing attempts
  - ensuring safe internet browsing habits

Preventive Measures

Robust Password Management
- Use complex, unique passwords for ALL accounts!
- Implement a password management tool!

Preventive Measures

Multi-Factor Authentication (MFA)
- Enforce the use of MFA across all church systems and accounts
- MFA adds an extra step of verification, such as a code sent to a registered mobile device
- This means that even if passwords are compromised, unauthorized access is prevented.
Preventive Measures

Secure Network Infrastructure

- Regularly update hardware and software, including firewalls and network equipment.
- Segment the church’s network to limit access to sensitive systems and data.
Protecting Against Cybercrime

Data Encryption
- Utilize encryption techniques, both at rest and in transit. – USE A VPN!
- Encrypt hard drives, backup files, and data transferred outside the organization.

Regular Data Backups
- Perform regular backups of critical data and store them securely, both onsite and offsite.
- Test the restoration process periodically.

Incident Response Plan
- Develop a comprehensive incident response plan to guide the church’s response in the event of a cyber incident.
- Include steps to:
  - contain the attack
  - notify relevant stakeholders
  - restore systems and data effectively.
Protecting Against Cybercrime

Ongoing Security Monitoring
- Implement robust security monitoring tools and practices to detect and respond to potential threats in real-time.
- Regularly review system logs, conduct vulnerability assessments, and perform penetration testing to identify weaknesses.

Collaborative Efforts & External Support
- Collaborate with other UM organizations, cybersecurity professionals, and local law enforcement.
- Share information, resources, and best practices to collectively strengthen cyber defenses.
Plan. Protect. Restore.

- You’ve planned...
  - Via education, training, audits, best practices, encryption, etc.
- You’ve protected...
  - Via security and insurance
  - Incidents are not inevitable. Let’s discuss restoring and recovering!

Goals for Response Plan

- Early identification & reporting
- Fast response
- Launch recovery efforts
- Continue operations
- Regulatory compliance
- Learn from the incident
Insuring Cyber Risk

Covers Two Main Obligations:
- Damage to your organization
- Obligations to others

- Ransomware + social engineering
- Business interruption + contingent business interruption (vendors)
- All data breaches: digital/paper/data (vendors)
- Regulatory fines + investigations
- Crisis management + legal counsel
- Recovery costs
- Forensic services
Threats

- Ransomware – easy to spot
- Social Engineering – easy to spot
- Malware & Viruses – may produce signs
- Probing for weakness
- Probing can be spotted by computer logs and security software
- An IT professional can help monitor activity and determine the source

Malware Warning Signs
Malware Warning Signs

- Unknown programs that open upon computer start-up
- Programs automatically connect to the internet
- Unusual activities like password changes
- Frequent pop-up windows: visit unusual sites, download antivirus/other software, etc.
- Changes to your home page
- Mass emails sent from your account
- Frequent crashes or unusually slow computer performance

Who Ya Gonna Call?

- IT department or provider
- Law enforcement
  - Local police
  - FBI
- Cyber insurance carrier
- Lawyers
- Financial institution
- Those affected by the release of personal information
What Will IT Do?

- Identify the threat
- Contain the breach
- Identify what, if anything, was stolen
- Check for and remove malware (visible or hidden)
- Find the cause of the breach
- Restore the system (did you backup?)
- Evaluate and update cybersecurity and training
- Provide information to your lawyers, insurance carrier, and providers

Why law enforcement?
Why law enforcement?

- Chances of recovering funds are low
- Reporting to law enforcement is generally required by insurance
- Local law enforcement is obligated to help
- The Internet Crime Complaint Center (IC3):
  - IC3 is run by the FBI and can make referrals to other agencies
  - If a foreign entity is involved, the FBI has resources to help!
  - The FBI also builds a database of attacks

Insurance

- Report the claim to your agent or the company immediately
- The response is based on the terms and conditions of your policy
- Your insurance provider will:
  - Provide a panel of experts to help
  - Respond to your damage and third-party damage
  - Can pay for loss of income, ransomware, other business interruption
  - Can protect you if you are ultimately sued
Legal Help

- Should come from your insurance carrier – expertise
- Crucial if sensitive information was lost
- Most states have laws requiring that you notify people that their personal data was lost – insurance can help
- There may be lawsuits coming your way

Your Bank
Your Bank

- Avoiding such losses is the best strategy
- The average loss to social engineering is $130,000
- Immediately contact your financial institution
- Ask them to contact the financial institution that received the funds
- There is a very slim chance the money can be recovered, or the transfer prevented

Third-Party Information

- Most states have requirements that you notify people in the event of the unauthorized release of personal information
- Always know your state rules if you keep such information in your system
Third-Party Information

- Work with your IT department, lawyers, law enforcement, and insurance company
- They will let you know what to say, remedies to offer, and timing
- Delayed reporting may be allowed to protect an investigation

Conclusion

- Plan and prepare in advance
  - Improved security
  - Proper insurance protection
  - Faster response to incidents
  - Greater chance of recovery and improvement
- The bigger you are, the bigger the need
- You are a target no matter how small
- Work with experts at all levels to plan, protect, and restore
Please complete the survey and help us improve our webinars!