Cyber Criminals in the Church

A Whopper of a Tale

Presented by Steven D. Goodspeed and Mark Francis Juba

THE CHURCH LAWYERS

Learning Objectives

- A Recent Ransomware Attack on a Church Client and Lessons Learned
- Identify and Explore Cybercrime and the Types of Malware Used to Commit Cybercrimes Against Churches
- Measures and Practices to Protect IT Systems and Usage at Your Church

Cyber Criminals in the Church

What happened?!

- Late October 2020, emails were sent to many employees containing what appeared to be a legitimate invoice for services/product rendered.
- One employee, wanting to be helpful, opened the invoice and set in motion the particular Ransomware.

Cyber Criminals in the Church

- Two weeks after the email was opened, the ransomware had been replicating itself like a virus throughout the entirety of the organization.
- Systems were brought down in mid-November and many, many copies of a ransom note were saved all over the network and printed out on system printers, etc.
- The church contacted our law firm and we involved insurer and filed a criminal report with the FBI.

Cyber Criminals in the Church

- Soon, we found ourselves at our law office with church representatives and two FBI agents.
- Each field office specializes in a particular kind of ransomware. The ransomware at issue was called Revil and it is an organization and program based out of Russia.
- Criminal Franchise “business” model including leased software.
- Scope of Problem and Peak Won’t Be for Another 3-5 Years.

"I'm no expert, but I think it's some kind of cyber attack!"

Cyber Criminals in the Church

I. Cybercrime – the Basics

- What is "Cybercrime"?
  - *Generally*: **any criminal activity that involves a computer, networked device, or a network.**
- Council of Europe Convention on Cybercrime (United States is a signatory) defines cybercrime as:
  - "a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements."

Cyber Criminals in the Church

II. Department of Justice Three (3) Categories of Cybercrime

(1) crimes in which the computing device is the target (*e.g.*, to gain network access);

(2) crimes in which the computer is used as a weapon (*e.g.*, to launch a denial-of-service (DoS) attack); and

(3) crimes in which the computer is used as an accessory to a crime (*e.g.*, using a computer to store illegally obtained data).

Cyber Criminals in the Church

III. Common Examples of Cybercrimes (non-exhaustive)

- **Harassment**
  - Cyberbullying
  - Cyber-harassment
  - Cyber-stalking
- **Phishing**
  - Fake emails
  - Fake businesses
  - Login and password “tricks”
- **Pharming**
  - Redirection to phony websites (or to hijack company domain)

Cyber Criminals in the Church

III. Common Examples of Cybercrimes Cont'd…

- **Fraud**
  - Scheme(s) to give money or property to people
  - Fake bidding on fake bid sites and/or items
- **Identity-Theft**
  - Key-logging
  - Tracking to gather your personal data
- **Cyber-Terrorism**
  - the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.
- **Malware***

Cyber Criminals in the Church

IV. Types of Malware (non-exhaustive)

- Adware (spyware)
- Viruses
- Worms
- Trojan Horses
- Rootkits
- Spam

AND …

Cyber Criminals in the Church

IV. Types of Malware Cont'd…

Ransomware*

- **Illegal computer software that stops a computer (or network) from working or prevents the user from getting information until they pay money or other certain funds.**
  - **Commonly used in coordination with other malware types to infect a computer and/or network (*e.g.*, spam).**

Cyber Criminals in the Church

Actually, this church had done many things right before the ransomware attack occurred:

- Encrypted Backups (Rubrick)
- Antivirus (SentinelOne)
- Email Phishing Awareness (KnowBe4)
- Cyberliability Insurance Policy

Cyber Criminals in the Church

V. Added Measures to Help Protect Against Cybercrimes

- **Firewalls**
  - Hardware device that blocks access to the network
  - Software that blocks access to individual computer
- **Antispyware software**
  - Prevents adware and spyware from installing onto network and/or computers
- **Full Security Suite**
  - Multiple programs and protections – often constantly updated and upgraded; often include new protection programs as available

Cyber Criminals in the Church

V. <u>Added Measures to Help Protect Against Cybercrimes, cont'd</u>

- **Multi-Factor Authentication**

AND

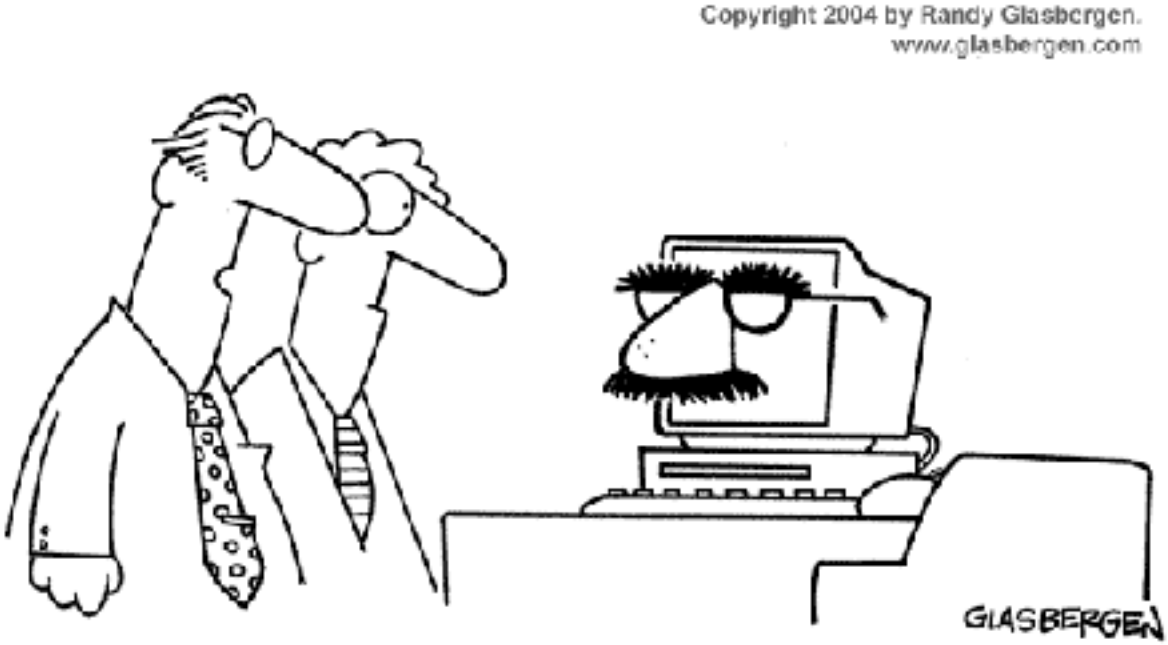
- **Internal Organizational Controls***
  - ***Employee Education***
  - ***Security Surveillance***
  - ***Activity Monitoring***
  - ***Training***

Cyber Criminals in the Church

Colonial Pipeline Company

- Ransomware attack
- Nearly $5m paid
- Operator of one of nation's largest pipelines
- Precautionary shut down, work to restore systems continues
- 2.5m barrels daily or 45% of east coast fuel supply was at risk

- Ultimately, the criminals picked the wrong church to mess with really.
- Cyberliability Insurance (necessary but not sufficient)
  - Not so much to pay a ransom but allows specialized law firms to be hired to manage the donor data breach notification laws which are unique to different states as well as help manage crisis communication and public relations aspect
  - Baseline controls (red the fine print)



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

THE CHURCH LAWYERS