Cybersecurity and the parish:
Securing systems and protecting parishioners in the age of ransomware

Theo Nicolakis | Metropolis of Atlanta Clergy-Laity | June 23, 2023
Sorry, ignorance isn’t bliss:
We’re here to scare you so you do something after this session
What are our Goals?

• Drop the veil of Naïveté: Ignorance is danger
• Educate, educate, educate
• Communicate what we’re doing nationally
• Point you to resources and action
• Embrace the mantle of leadership
Our initiative

• Archdiocese and Metropolis joint effort.
• CISA and Homeland Security
• Leadership 100 support. THANK YOU L100!
How will we do this?

Three parts

- Cybersecurity portion
- Physical Security
- Action steps with Q&A
The power of the phalanx is unity: The phalanx only works when everyone is locked together.
Threat Landscape: It’s not good
Cybersecurity Threats

Magnitude of the threat

• Of the cyber insurance claims made in the past 7 years, 73% were related to data breaches, incident response, and crisis management.

• Small and medium-sized enterprises (SMEs) have become a prime target for cyber attacks, with over 56% of claims originating from companies with less than 25 million dollars in revenue.

Source: https://thecyphere.com/blog/cyber-insurance-statistics
Cybersecurity Threats

Magnitude of the threat

- The average cost of a cyber insurance claim for an SME is approximately $345,000.
- Ransomware was the main cause of recovery expense losses, accounting for 81% of such claims.
- The frequency of cyber insurance claims has increased by 100% in the past three years.

Source: https://thecyphere.com/blog/cyber-insurance-statistics
Cybersecurity Threats

You should be getting really worried right about now

• **Ransomware is common (and lucrative).** In 2020, 1 in 6 businesses that fell victim to cyberattacks faced ransomware, and about half of them paid up the ransom.

• **Cybercrime reports nearly doubled.** The FBI’s Internet Crime Complaint Center (IC3) saw a 69 percent increase in the number of cybercrime reports it received in 2020 compared to 2019. On average, the FBI received 2,000 cybercrime reports per day in 2020.

Source: https://www.security.org/insurance/cyber/statistics/
Cybersecurity Threats

You should be getting really worried right about now

• **Data breaches affect personal data.** In 2020 alone, data breaches exposed over 37 billion personal records, 82 percent of which came from only five breaches.4 Data breaches affect not only companies and organizations, but also the people whose information is in the exposed records.

• **Identity fraud causes serious losses.** Identity fraud losses in 2020 cost its 49 million victims $56 billion in total. That breaks down to $1,100 per victim.5

• **Cyber attacks are the most common:** For those that are slightly to somewhat familiar with cyber insurance, 70 percent have experienced a cyber attack, followed by identity theft at 69 percent, cyberbullying at 64 percent, and cyber extortion at 69 percent.

Source: https://www.security.org/insurance/cyber/statistics/
How does it hit home?
Cyberattack on food giant Dole temporarily shuts down North America production, company memo says

Ransomware attack closes schools in Nantucket

Ransomware attack delays patient care at hospitals across the U.S.

Lacroix manufacturing facilities shut down following cyberattack

French electronics manufacturer Lacroix closed three factories as a result of a cyberattack they "Intercepted" over the weekend, the company has announced on Monday.
But We’re OK

We’re a Church RIGHT?
Other church officials spoke to the AP about the hacking on condition of anonymity, saying they did not have authorization to speak to the media.

Bartholomew, who is 78, does not use email, those church officials told AP. But his aides do, and the Secureworks list spells out several attempts to crack their Gmail accounts.

Among them were several senior church officials called metropolitans, who are roughly equivalent to archbishops in the Catholic tradition. Those include Bartholomew Samaras, a key confidante of the patriarch; Emmanuel Adamakis, an influential hierarch in the church; and Elpidophoros Lambriniadis, who heads a prestigious seminary on the Turkish island of Halki. All are involved in the church's efforts to demonstrate its growing power in the region.
LONDON (AP) — The Russian hackers indicted by the U.S. special prosecutor last month have spent years trying to steal the private correspondence of some of the world's most senior Orthodox Christian leaders.

The targets included top aides to Ecumenical Patriarch Bartholomew I, who often is described as the first among equals of the world's Eastern Orthodox Christian leaders.

association with a conflict between Ukrainian military forces and Russia-backed separatists in eastern Ukraine.

The AP's evidence comes from a hit list of 4,700 email addresses supplied last year by Secureworks, a subsidiary of Dell Technologies.

The AP has been mining the data for months, uncovering how a group of Russian hackers widely known as Fancy Bear tried to break into the emails of U.S. Democrats, defense contractors, intelligence workers, international journalists and even American military wives. In July, as part of special counsel Robert Mueller's ongoing investigation into Russian interference in the 2016 U.S. election, a U.S. grand jury identified 12 Russian
Worshipers targeted by gift card scam

By: Colleen Tressler, Consumer Education Specialist, FTC

We’re seeing a new spin on gift card scams. This time, scammers are pretending to be a pastor, rabbi, priest, imam, or bishop. They’re asking worshipers for gift card contributions for a worthy cause. Appeals are often made by email, but we’ve heard people are also getting texts and phone calls, too.
Hi,

How are you and your family doing? I hope this email finds you all in good health and I hope you are keeping safe, hopefully 2022 will be the end of the pandemic. Let me know if you receive my message, I need a quick favor from you, I’ll be looking forward to hearing back from you.

Thank you
Fr. John
Let’s look at real examples and horror stories
Be smart. Don’t be the next victim

- Orthodox Christian organizations targeted
- Archdiocese and other organizations have had sophisticated phishing schemes targeting treasurers and finance department to exfiltrate tens of thousands of dollars.
- Strong internal controls protected the Archdiocese.
- Sheer luck (divine intervention!) saved the others.
> Path to Antivirus Product: Get List
  > Trend Micro
  > Malware Bites

> Get System info
  > Get Trusted Domains
  > Net Group Domain Admins

> Search network devices
  > Secretary-Computer
  > Main Server
  > Accountant Computer

> Net View All
  > 10.0.0.1 Arris Surfboard Modem
  > 10.0.0.2 Netgear Router
  > 10.0.0.3 Netgear Wireless Access Point
**Execution**

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Information-gathering objective.
Dear Chancellor,

I am in a meeting. Download the attached file immediately and look at the budget numbers. Please let me know that you received it.

Metropolitan Megapsareas

Metropolis of Phishing | 123 Cyberduck Lane | (220) 222-2222

P.S. Immediately means immediately.
Some of our initiatives

This is what’s protected us

• Securing and central management of all Metropolis computers and networks
• 24/7/365 Managed endpoint detection and response
• Protective DNS to prevent access to malicious sites and detect anomalous behavior
• 24/7/365 monitoring and analysis of GOA and Metropolis networks and systems
• 2-factor authentication securing key systems and remote access
• Standardization of hardware, operating systems, and white-list software
Some action items to ponder
Key Things You Can Do

Pull out your iPhone

Create a security culture:
- Talk security pulpit, bulletin, email
- Talk about these security issues and scams from the pulpit—Education and communication is your primary defense.
- Publish bulletin inserts developed by the Department of Internet Ministries [https://blogs.goarch.org/internet-ministries](https://blogs.goarch.org/internet-ministries)

Define your protection bubble:
- Implement Parish-owned M365 or Google Workspace for all emails.
- Adopt and enforce corporate devices — Sunset use of all personal emails and device.
- Audit assets: Know WHAT to protect.
- Audit accounts: Know WHO to protect.
Key Things You Can Do

Pull out your iPhone

Minimize your exposure risk:
- Remove emails from parish web site—use online forms
- Beware what you share on social media

Protect:
- Install next generation anti-virus (EDR software) on every system and NextGen Firewall
- Implement MFA everywhere
- Use strong passwords—minimum 16 characters (use phrases) and password lockers
- Implement Protective DNS (Cisco Umbrella, OpenDNS)
- Define secure
- Establish a security committee
- Meet with local law enforcement (police and fire)
Resources to Reference

Pull out your iPhone and take a picture

CISA’s protecting houses of worship resources:  
https://www.cisa.gov/topics/physical-security/protecting-houses-worship

Cybersecurity Performance Benchmark Goals:  
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

Nonprofit Security Grant Program (NSGP): Provides funding support for target hardening and other physical security enhancements and activities to nonprofit organizations that are at high risk of terrorist attack:  
https://www.fema.gov/grants/preparedness/nonprofit-security
And one more thing...
Special Thanks

- Archbishop Elpidophoros
- Metropolitan Alexios
- Fr. George Tsahakis
- Fr. Nektarios Papazafiropoulos
- Elaine Allen
- **HUGE thanks** to Leadership 100