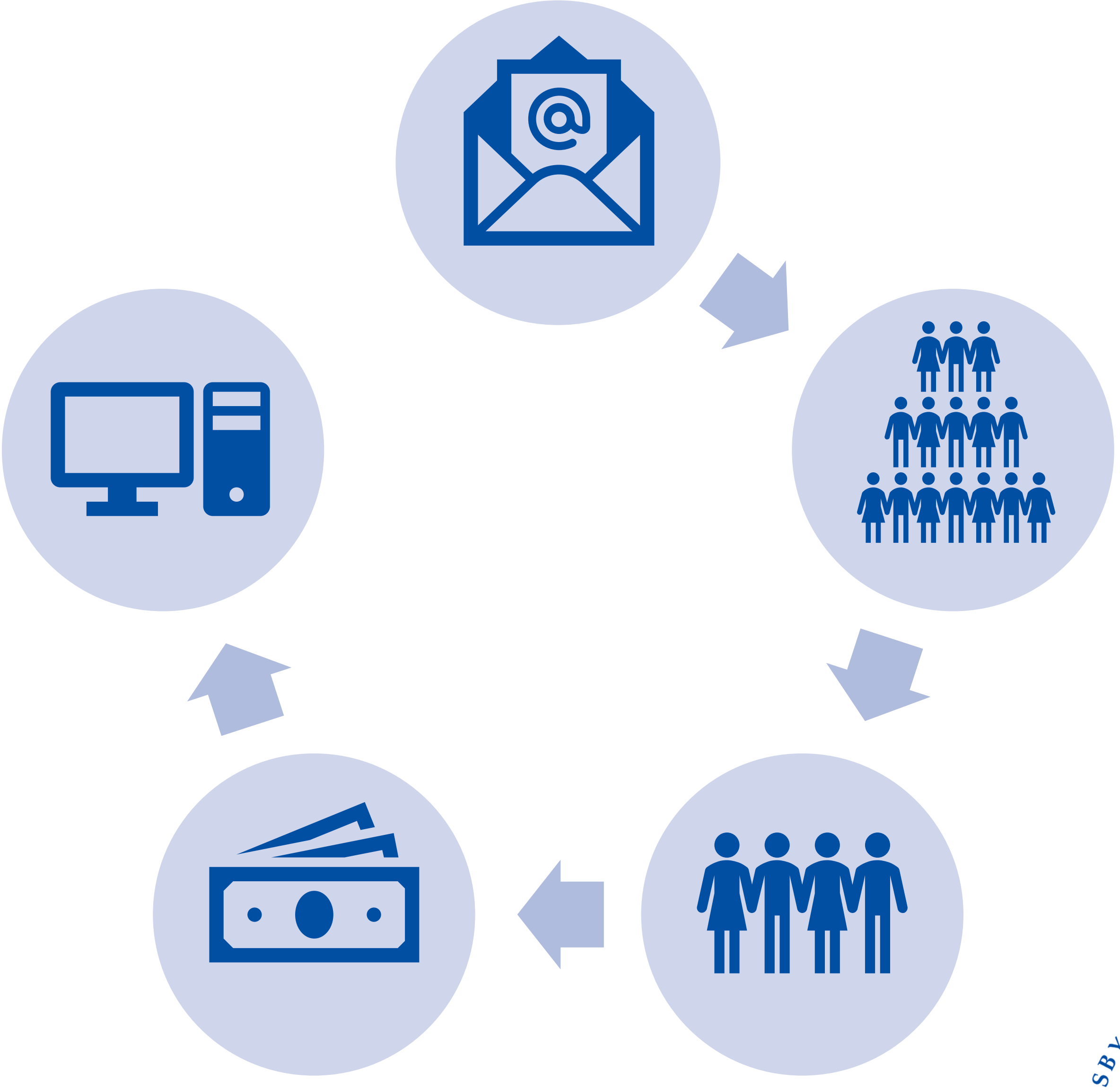
Cybersecurity

Presented by Ian Hall

Presbyterian Church (USA)

Presbyterian Church (USA)

A Call to Action



Cybersecurity

- Cybersecurity – A Definition
- What Is Cybercrime
- Common Cybercrime Activities
- Potential Impact of Cybercrime
- Threat Assessment
- Safeguarding
- Proactive Security Measures
- Shadow IT
- Training & Awareness
- Cyber Safety Tips
- Incident Response Planning
- What Do We Do After A Cybersecurity Incident?
- Resources

Cybersecurity – A Definition

The practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access

The act of safeguarding sensitive information and ensuring the continuity of operations

What is Cybercrime ?

Criminal activities carried out using digital technology and the internet

The Verizon **2023** Data Breach Report analyzed **16,312** security incidents and **5,199** confirmed data breaches.

The majority of breaches **(83%)** involve **external actors**, with the vast majority **(95%)** being **financially motivated**.

Almost three-quarters **(74%)** of all breaches include the **human element** including error, privilege misuse, use of stolen credentials or social engineering.

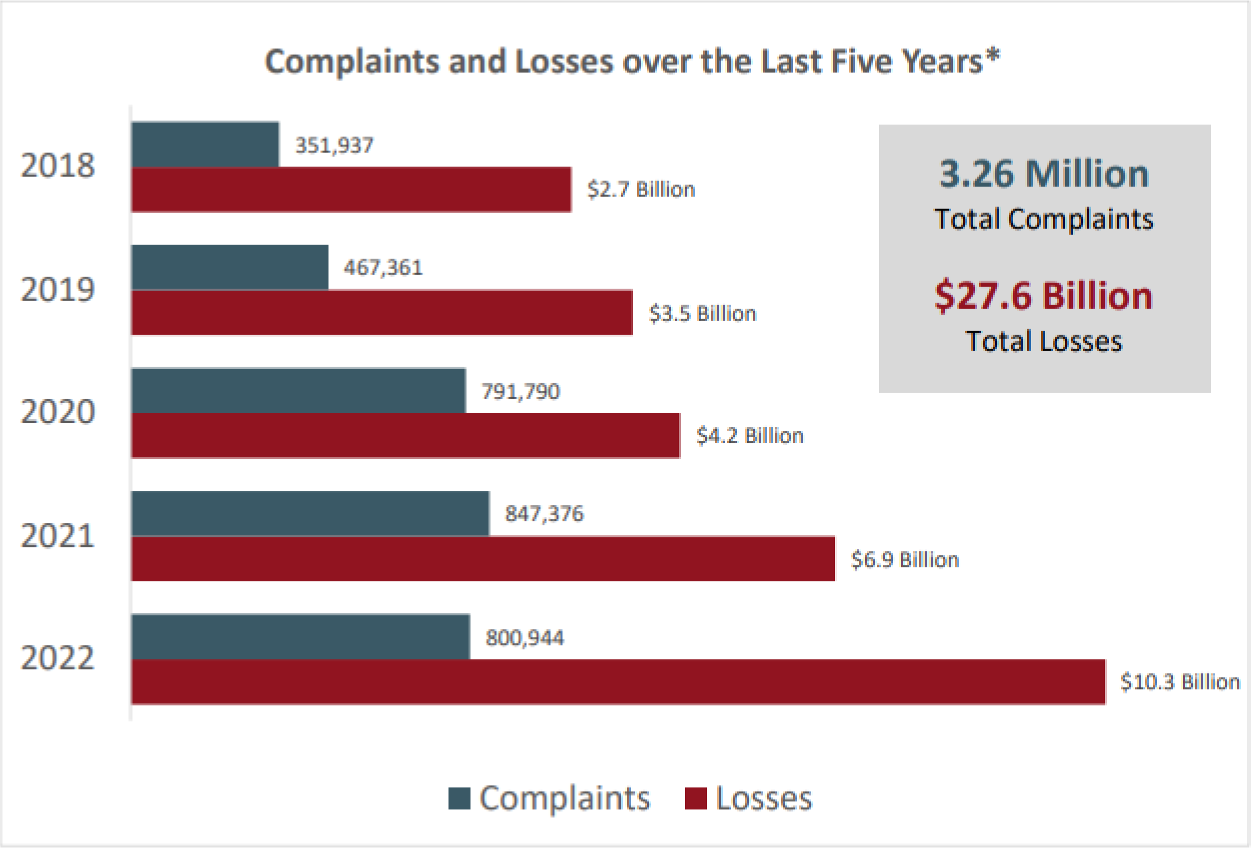
According to a report by TechSoup, **58%** of **non-profits** experienced a **cybersecurity incident** in **2021**, and **71%** of those incidents resulted in a **financial loss.**

According to a report by the National Cyber Security Alliance, **95%** of all cybersecurity breaches are caused by **human error**.

PRESBYTERIAN CHURCH (USA)

Internet Crime Complaint Center (IC3)
FBI STATISTICS

Over the last five years, the IC3 has received an average of 652,000 complaints per year. These complaints address a wide array of internet scams affecting victims across the globe.

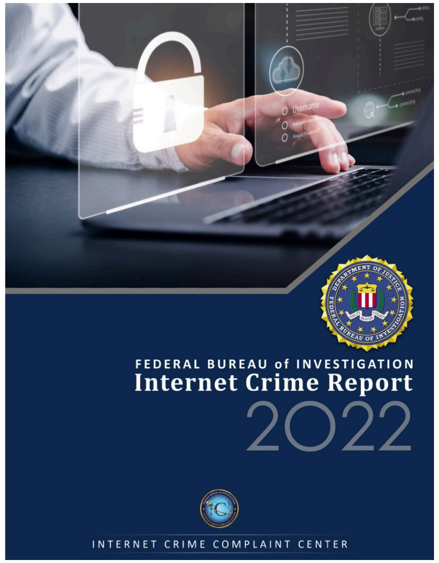


$10.3 Billion
Victim losses in 2022

2,175+
Average complaints received daily

651,800+
Average complaints received per year (last 5 years)

Over 7.3 Million
Complaints reported since inception


FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2022
INTERNET CRIME COMPLAINT CENTER

https://www.ic3.gov

Common Cybercrime Activities

Hacking

Hacking refers to the act of gaining unauthorized access to computer systems, networks, or digital devices for the purpose of manipulating, stealing, or altering data, as well as for various other illicit activities.

Malware

Malware is any type of software or code specifically designed with malicious intent to harm, compromise, or exploit computer systems, networks, or digital devices without the knowledge or consent of the owner or user.

Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's data or locks them out of their own system, rendering the data or system inaccessible.

Common Cybercrime Activities

Phishing

Phishing is a cyberattack technique that involves tricking individuals into revealing sensitive or confidential information, such as login credentials, personal information, or financial details, by posing as a trustworthy entity or person.

Spear Phishing / Social Engineering

Spear phishing is a highly targeted and personalized form of phishing attack in which cybercriminals or attackers tailor their deceptive messages to a specific individual, organization, or group of people.

Potential Impact of Cybercrime

- Financial Consequences
- Reputational Damage
- Legal and Compliance Issues
- Data Breaches and Privacy Concerns

Threat Assessment

- The Nonprofit Technology Enterprise Network (NTEN) suggests that the first step in assessing your nonprofit's data risks is to take inventory of all the data your nonprofit collects and identify where it is stored.
    - *What data do we collect about people?*
    - *What do we do with it?*
    - *Where do we store it?*
    - *Who is responsible for it?*
- Are the data your nonprofit maintains "protected" or "confidential"?
- What is the actual risk?

Free Security Assessment

Microsoft

Microsoft’s Tech for Social Impact team has a goal to meet you where you are on your cloud and security journey, by supporting you in mitigating security risks to your organization’s digital environment.

https://nonprofits.tsi.microsoft.com/EN-US/security-assessment

Safeguarding

- Utilize Current Hardware and Operating Systems
- Regular Software Updates and Patch Management
- Anti-Malware and Antivirus Software
- Firewalls and Intrusion Detection Systems

techsoup

https://www.techsoup.org

TechSoup provides technical support and technological tools to other nonprofits.

Proactive Security Measures

Strong Passwords	Create a strong and unique passphrase for each online account and change those passphrases regularly.
Multi Factor Authentication (MFA)	Set up multi factor authentication on all accounts that allow it.
Password Management Tools	Establish best practices while storing and managing passwords.

Proactive Security Measures

Backup

- Data, System Images, & Configurations
- Test Backups
- Keep Backups offline / offsite

Data Encryption

- Utilize encryption techniques to protect sensitive data, both at rest and in transit.
- Encrypt hard drives, backup files, and any data transferred outside the organization.

Proactive Security Measures

Security Policies and Procedures

- Written guidelines and protocols for protecting digital assets and data
- Ensuring confidentiality, integrity, and availability of IT resources
- Establish the overarching framework and rules
- Provide detailed instructions for implementation and adherence

Access Control

- Regulating and restricting access to computer systems, networks, data, or resources
- Authentication: Verifying user identities
- Authorization: Determining and granting specific access permissions
- Accountability: Tracking and recording user actions

PRESBYTERIAN CHURCH (USA)

Shadow IT?

- Shadow IT refers to information technology (IT) systems, software, applications, or services that are used within an organization without the explicit approval, oversight, or knowledge of the IT department or official IT policies.

Employee Training and Awareness

Does your organization provide cybersecurity training to employees on a regular basis?

If so, is the training mandatory?

Did employees learn about areas in which their behavior is a factor?

Are employees allowed to use their personal devices to access organizational emails and business files?

FBI Cyber Safety Tips

Keep systems and software up to date and install a strong, reputable anti-virus program.

Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.

Examine the email address in all correspondence and scrutinize website URLs before responding to a message or visiting a site.

PRESBYTERIAN CHURCH (USA)

FBI Cyber Safety Tips

Don’t click on anything in unsolicited emails or text messages.

Be cautious about the information you share in online profiles and social media accounts.

Incident Response Plan

Purpose

“The Presbyterian Church (U.S.A.), A Corporation (“A CORP.”) Cyber Incident Response Plan (“IRP”) provides a consistent framework for A CORP. to respond to a cybersecurity event. The IRP will serve as a guide to facilitate a response in a systematic manner to cybersecurity events and is designed to:

(a) prevent or minimize disruption of critical information systems;
(b) minimize loss or theft of sensitive or critical information; and
(c) quickly and efficiently remediate and recover from security events.”

PRESBYTERIAN CHURCH (USA)

Incident Response Plan Outline

a) Preparations

b) Incident Response Team

c) Cyber Incident Response Preparation

d) Initial Reporting of Potential Events

e) Authority of Incident Response Team

f) Incident Response Process
   - Identification & Assessment
   - Containment, Eradication & Recovery
   - Communication & Notification
   - Special Considerations
   - Final Steps/Preservation of Records

Partnership

- Security Operation Center
- Cyber Insurance Response Team

PRESBYTERIAN CHURCH (USA)

What Do We Do After a Cybersecurity Incident?

RESTORE BACKUPS

INVESTIGATE

COMMUNICATION / NOTIFICATION

PRESBYTERIAN CHURCH (USA)

Cyber Insurance

Collaborate with a knowledgeable insurance agent or broker.

Work together to assess your nonprofit's specific cyber exposures.

Tailor the insurance coverage to address these unique risks.

Resources

VERIZON

THE NONPROFIT TECHNOLOGY ENTERPRISE NETWORK (NTEN)

NATIONAL CYBER SECURITY ALLIANCE