RBC Cardinal Health DENVER

JULY 9-12, 2025

NCPA®

NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

Ctrl+Alt+Secure: Cybersecurity Practices for Safeguarding Your Pharmacy

Scotty Sykes, CPA, CFP®, Vice President, Sykes & Company, P.A.

Chris Sykes, MCSA, M.S., Director of IT, Sykes & Company, P.A.

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

RBC Cardinal Health DENVER
JULY 9-12, 2025

Disclosure Statement

There are no relevant financial relationships with ACPE defined commercial interests for anyone who was in control of the content of the activity.

Pharmacist and Technician Learning Objectives

1. Review best practices for preventing a cybersecurity incident.
2. Outline an action plan for quickly responding to a data breach.
3. List ten steps to take in the event of a security breach.

Speakers

Scotty Sykes, CPA, CFP®

Vice President

Sykes & Company, P.A.

Chris Sykes, MCSA, M.S.

Director of IT

Sykes & Company, P.A.

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

Pharmacy Cybersecurity Threats: Real-World Scenarios

Top Threats Facing Pharmacies

- Ransomware
- Malware
- Phishing
- Stolen or compromised credentials
- Social engineering
- Threats often overlap:
    - Example: most ransomware incidents begin as phishing

2024 Attack on Change Healthcare

- Lack of ***multi-factor authentication*** gave a ransomware group access to ***compromised credentials***.
- Use of ***compromised credentials*** allowed the ransomware group to gain remote access to Change Healthcare Citrix portal.
- Citrix portal access gave the ransomware group ability to move laterally within the system.

Independent Pharmacy

- “Client” reaches out to accounts payable via email looking to pay a “vendor”
- “Admin personnel” replies stating that they can make the payment but may be later until they can get to it
- “Client” approves and says thanks and copies outsourced accountant
- After approval from “client” & “admin”, third-party accountant ***notices a discrepancy*** in the account numbers and also notices unusual amount

Independent Pharmacy

- Third-party accountant verifies via phone or text as follow-up email doesn’t ***feel*** right
- Phone call with client confirms that their email was hacked and accounts payable request from Admin Personnel was incorrect/based on fraudulent email
- **Critical Gaps Identified:**
  - Business Email Compromise on two accounts
  - Checks and balances
- **Outcome:** Payment is not processed!

Knowledge Check

What was this pharmacy owner the victim of?

A) Stolen or compromised credentials

B) Phishing

C) Social engineering

D) All of the above

Knowledge Check

What was this pharmacy owner the victim of?

A) Stolen or compromised credentials

B) Phishing

C) Social engineering

D) [✓ All of the above]

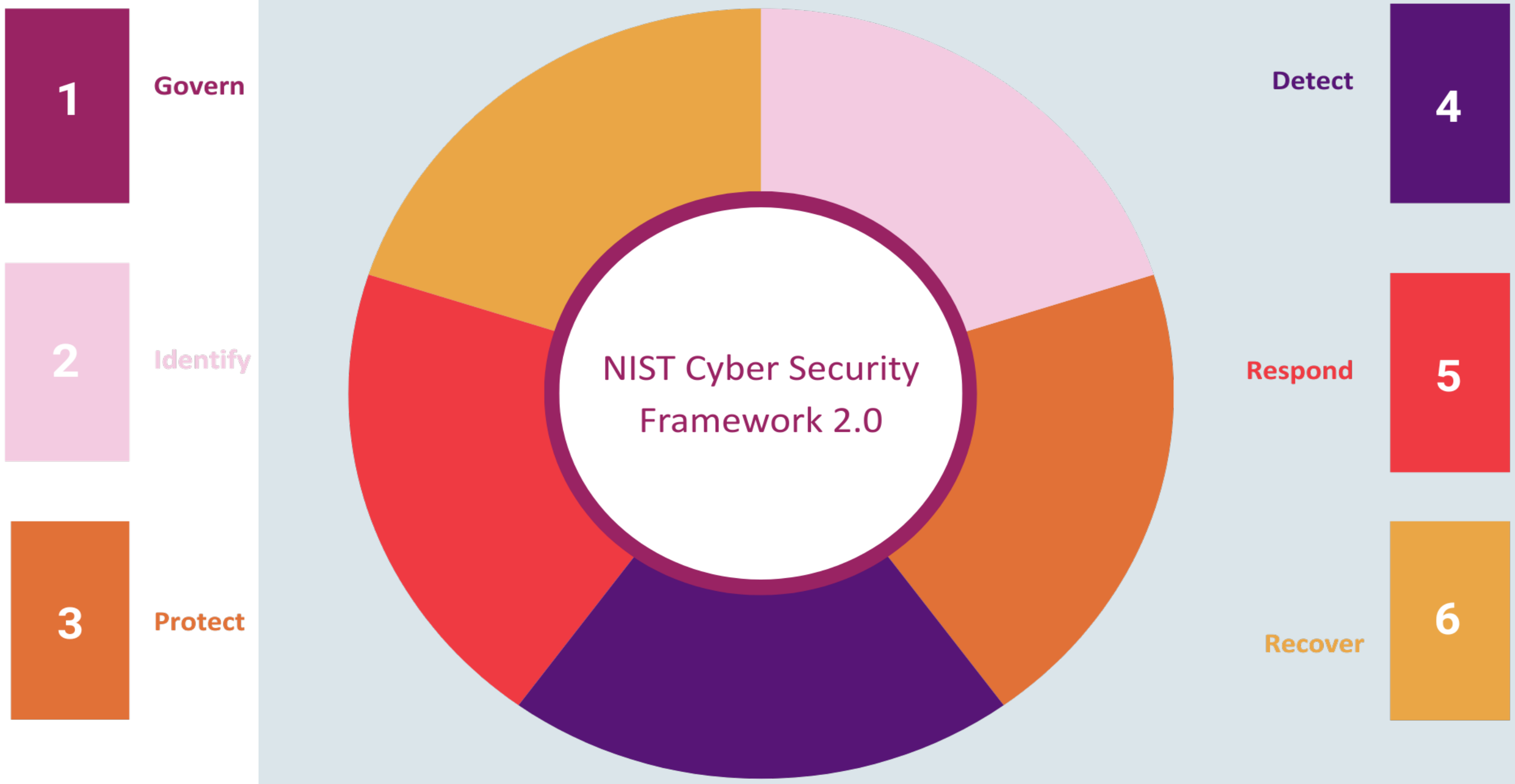
The Incident…

- Hacker utilized a phishing attack to gain email access
- Credentials were now compromised
- Hacker then utilized social engineering to try to funnel a large sum of money to their bank account in the form of an AP request
- **Red Flags:**
  - Mismatching invoice numbers
  - Large sum of money requested

NIST CSF:
A Framework for Safeguarding Your Pharmacy

NIST CSF At A Glance

- Guidelines developed by the National Institute of Standards and Technology (NIST)
- Proactive risk management
- Third-party risk awareness
- Flexible and scalable
- HIPPA compliant



NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

NIST CSF Deep Dive

Govern

Strategy, Policy & Accountability

Govern

Helps you establish and monitor your pharmacy’s cybersecurity risk management strategy, expectations, and policy.

- Do you have acceptable use policies in place for the pharmacy and for employee-owned devices accessing business resources?
- Have employees been educated on these policies in the last 12 months?

Identify

Know Your Digital Environment

Identify

Before you can protect your assets, you need to identify them.

- The HHS Office for Civil Rights recently emphasized the need for a detailed IT inventory and network map in its proposed HIPAA update. NCPA has commented on this: ncpa.co/pdf/2025/advocacy/ncpa-hipaa-comments.pdf
- What are the most critical business assets we need to protect?
  - Data, hardware, software, systems, facilities, services, people, etc.
- What technologies or services are personnel using to accomplish their work?
  - Are these services or technologies secure and approved for use?

Protect

Safeguard Systems and Data

Protect

Supports your ability to use safeguards to prevent or reduce cybersecurity risks.

- Are we restricting access and privileges only to those who need it? Are we removing access when they no longer need it?
- How are we securely sanitizing and destroying data and data storage devices when they are no longer needed?

Protect

Safeguard Systems and Data

Backups

- Originally served to protect against hardware failure or physical damage.
- Now, backups are equally critical to defend against ransomware, which can encrypt or lock access to files.
- A good backup can limit downtime if such an attack occurs
- Eliminates a single point of failure

Protect

Safeguard Systems and Data

Backups

Determine what needs to be backed up and why:

- Dispensing records
- Email
- Documents

- 3, 2, 1 Backup strategy
- Encrypted at rest and in transit
- Testing restores
- Daily and Often...

Endpoint Protection

Protect

Safeguard Systems and Data

- Secure systems and software hygiene
- Antivirus updates and anti-malware software installed
- Endpoint detection and response solutions

Enabling Multi-Factor Authentication (MFA)

Protect

Safeguard Systems and Data

Drastically reduces risk even if passwords are compromised.

- Multi-factor authentication on all pharmacy systems
- Authenticator methods:
  - SMS (other options if available)
  - App
  - Passkeys
  - Biometrics

Protect

Safeguard Systems and Data

Policies and Procedures

- Safe email and internet use protocols
- Vendor and third-party management
- Physical security measures:
  - Device lockout, server room access, etc.

Protect

Safeguard Systems and Data

Network Security

- Firewalls, segmented networks, and secure wi-fi protocols.
- Regularly audit your network for vulnerabilities.
- Restrict access based on roles.
- Risk assessment.
- Penetration testing.

Protect

Safeguard Systems and Data

The Human Firewall: Team Readiness & Engagement

- Training pharmacy staff.
- Phishing simulations and drills.
- Creating a culture of reporting and vigilance.
- Role-based responsibilities in case of breach.

Detect

Provides outcomes that help you find and analyze possible cybersecurity attacks and compromises.

Detect

Spot Threats Quickly

- Do the devices that are used for our business, whether business-owned or employee-owned, have antivirus software installed?
- Do employees know how to detect possible cybersecurity attacks and how to report them?

Respond

Respond

When a Breach Occurs

Supports your ability to act regarding a detected cybersecurity incident.

- Do we have a cybersecurity incident response plan?
    - If so, have we practiced it to see if it is feasible?
- Do we know the key internal and external stakeholders and decision-makers are who will assist if we have a confirmed cybersecurity incident?

Knowledge Check

Before responding to a cybersecurity incident, what should a pharmacy owner be mindful of?

A) Script management system protocols

B) What technologies or services are personnel using to accomplish their work

C) Are there any antivirus updates and anti malware software that needs to be installed

D) All of the above

Knowledge Check

Before responding to a cybersecurity incident, what should a pharmacy owner be mindful of?

A) Script management system protocols

B) What technologies or services are personnel using to accomplish their work

C) Are there any antivirus updates and anti malware software that needs to be installed

D) All of the above

10 Steps to Take in the Event of a Security Breach

Dependent on script management system…

- Isolate affected systems to contain the breach
- Activate your incident response plan
- Notify your IT provider and/or cybersecurity team
- Preserve system logs and relevant evidence
- Coordinate internal communication and inform staff
- Determine the scope, cause, and potential impact
- Notify law enforcement and/or regulators as needed
- Notify affected individuals if unsecured PHI was disclosed
- Report the breach to the Secretary of HHS, if required under HIPAA
- Begin remediation, recovery, and conduct a post-incident review

Recover

Restore Operations & Learn

Recover

Restore assets and operations that were impacted by cybersecurity breach.

The goal is not to be breach-proof but to be ***breach-ready***.

- What are our lessons learned?
- How can we minimize the chances of a cybersecurity incident happening in the future?

Real-World Application: NIST CSF In Action

Independent Pharmacy

- “Client” reaches out to accounts payable via email looking to pay a “vendor”
- “Admin personnel” replies stating that they can make the payment but may be later until they can get to it
- “Client” approves and says thanks and copies outsourced accountant
- After approval from “client” & “admin”, third-party accountant ***notices a discrepancy*** in the account numbers and also notices unusual amount **(Detect)**

Independent Pharmacy

- Third-party accountant verifies via phone or text as follow up email doesn’t ***feel*** right **(Response process begins)**
- Phone call with client confirms that their email was hacked and accounts payable request was incorrect.
- Payment is not processed!
- **(Recover process begins)**

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

Knowledge Check

When the outside party notices a discrepancy in the account numbers and unusual amount, this is an example of?

A) Detect

B) Creating a culture of reporting and vigilance

C) Respond

D) All of the above

NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Knowledge Check

When the outside party notices a discrepancy in the account numbers and unusual amount, this is an example of?

A) Detect

B) Creating a culture of reporting and vigilance

C) Respond

D) All of the above

Questions?

Scotty Sykes

Vice President, Sykes & Company, P.A.

Chris Sykes

Director of IT, Sykes & Company, P.A.