GPS

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

Growth. Performance. Success.

2024 ANNUAL CONVENTION

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

Cybersecurity Readiness:

Lessons for Preparing for and Responding to a Data Breach

NCPA 2024 Annual Convention and Expo

Columbus, Ohio

Speakers

Justine Del Prete

Director of Sales & Marketing

Elpha Secure

Denise Ricardo

Cyber Program Manager

Bolton Street Programs

NCPA® NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

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. Discuss best practices for preventing a cybersecurity incident.
2. Outline an action plan to quickly respond to a data breach.
3. Describe the importance of engaging all pharmacy team members in cybersecurity readiness.

NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

What is Cyber Insurance?

Cyber insurance provides for business continuity and protection from financial hardship after a cyber incident. Many cyber insurance products also offer valuable risk mitigation tools and services for the insured to better protect their organization and build resiliency.

What it protects

Cyber insurance protects against financial losses from data breaches, cyberattacks, and digital liabilities.

Who it protects

The business, employees, customers, and the balance sheet!

Why we need it

Increasing number of cyber attacks on businesses of all sizes. No business is immune from today's threat landscape.

What's at stake?
The financial stability of every organization.

What is the problem facing small business?

Cyber insurers are increasingly requiring that cyber security controls be in place in order to obtain cyber insurance at a reasonable price with proper coverage. Larger organizations with a CISO, or a well resourced IT department in place, have the budget and technical sophistication to procure, implement and maintain proper security hygiene to meet the underwriting requirements of insurance carriers. However, small businesses typically do not have the technical capabilities to protect themselves, nor the budget to do so properly. This gap is only widening as the cyber threat landscape evolves and threat actors refine and improve their capabilities. Protecting a small business, with both insurance and security controls, is quickly becoming resource intensive and an economic burden.

Knowledge Gap

Lack of Technical Sophistication

Budget Constraints & Resources

NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Repercussions for Small Businesses (SMBs)

LS0

A single cyber attack can have a larger impact on a Main Street business than any other liability

60% of small businesses that suffer a cyber attack of any size go out of business within 6 months.

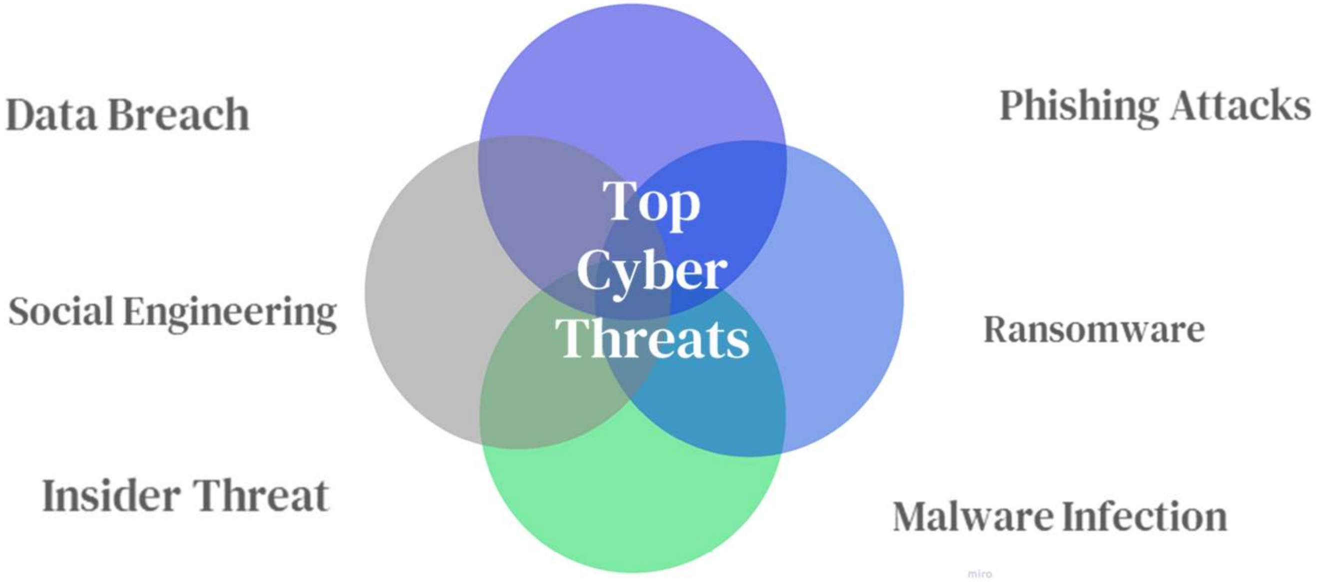
- Any internet connection or email can be the source of a compromise
- Any application or software a business uses can be the source of a compromise
- Many businesses have compromised credentials (e.g. logins//passwords) for sale on the Darkweb.

CLOSED
CLOSED
CLOSED
CLOSED
CLOSED
CLOSED

NCPA®
NATIONAL COMMUNITY
PHARMACISTS ASSOCIATION

What are the top cyber threats?

A cyber threat or cybersecurity threat is a malicious act intended to steal or damage data or disrupt the digital wellbeing and stability of an enterprise



Client Claim Story

Ransomware Attack on Pharmacy Systems

A small pharmacy chain experienced a ransomware attack that encrypted all of their patient records and billing information.

The attackers demanded a ransom of $50,000 in cryptocurrency. They also threatened to release the personal health information of patients if the ransom demand was not paid. Without access to their systems, the pharmacy couldn't process prescriptions or insurance claims, leading to significant business interruption.

Because the attackers exfiltrated the personal information of patients, the small pharmacy needed to incur the cost of notifying affected patients. After those patients were notified, one of the patients brought a lawsuit against them for failing to properly secure their personal health information.

NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Client Claim Story

Data Breach of Patient Information

A pharmacist’s email was compromised through a phishing attack, allowing hackers to access the pharmacy’s network. Sensitive patient information, including prescription details and personal health information (PHI), was stolen and later found for sale on the dark web. The pharmacy faced regulatory fines, legal fees, and costs for notifying affected patients and providing credit monitoring services.

Client Claim Story

Phishing Scam Leading to Financial Loss

An employee at a pharmacy received an email that appeared to be from a trusted vendor, requesting payment for an outstanding invoice. The employee unknowingly transferred $30,000 to a fraudulent account.

NCPA
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Client Claim Story

Malware Infection Disrupting Operations

A pharmacy’s computer system was infected with malware that corrupted their software, making it impossible to access patient records or process transactions. The pharmacy had to revert to manual processes, which significantly slowed down operations and led to a loss of customers.

NCPA®
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Client Claim Story

Vendor Breach Affecting Pharmacy Operations

A third-party vendor or business associate that provided software services to a pharmacy was breached, exposing the pharmacy's data. The pharmacy had to manage the fallout, including notifying patients, dealing with regulatory bodies, and handling public relations.

.

Client Claim Story

Social Engineering Fraud

A pharmacy manager received a phone call from someone posing as a bank representative, claiming there was an issue with the pharmacy's account. The manager provided sensitive information, which was then used to make unauthorized transactions, resulting in a significant financial loss.

NCPA
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

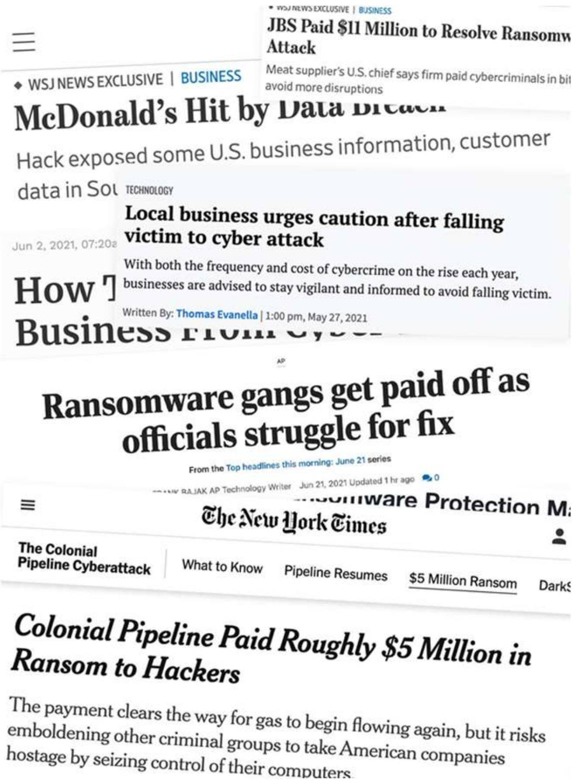
Client Claim Story

Insider Threat

A disgruntled former employee accessed the pharmacy's network using still-active credentials and deleted critical patient records. The pharmacy had to spend considerable time and resources to restore the data and secure their systems against future insider threats.

NCPA
NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

The path forward is clear for ALL Enterprises



WSJ NEWS EXCLUSIVE | BUSINESS

JBS Paid $11 Million to Resolve Ransomw Attack

Meat supplier's U.S. chief says firm paid cybercriminals in bit avoid more disruptions

WSJ NEWS EXCLUSIVE | BUSINESS

McDonald's Hit by Data Breach

Hack exposed some U.S. business information, customer data in Sou

Jun 2, 2021, 07:20a

How T Business From Cyber

TECHNOLOGY

Local business urges caution after falling victim to cyber attack

With both the frequency and cost of cybercrime on the rise each year, businesses are advised to stay vigilant and informed to avoid falling victim.

Written By: Thomas Evanella | 1:00 pm, May 27, 2021

AP

Ransomware gangs get paid off as officials struggle for fix

From the Top headlines this morning: June 21 series

RAJAK AP Technology Writer Jun 21, 2021 Updated 1 hr ago

Ransomware Protection M

The New York Times

The Colonial Pipeline Cyberattack | What to Know | Pipeline Resumes | $5 Million Ransom | Dark

Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clears the way for gas to begin flowing again, but it risks emboldening other criminal groups to take American companies hostage by seizing control of their computers

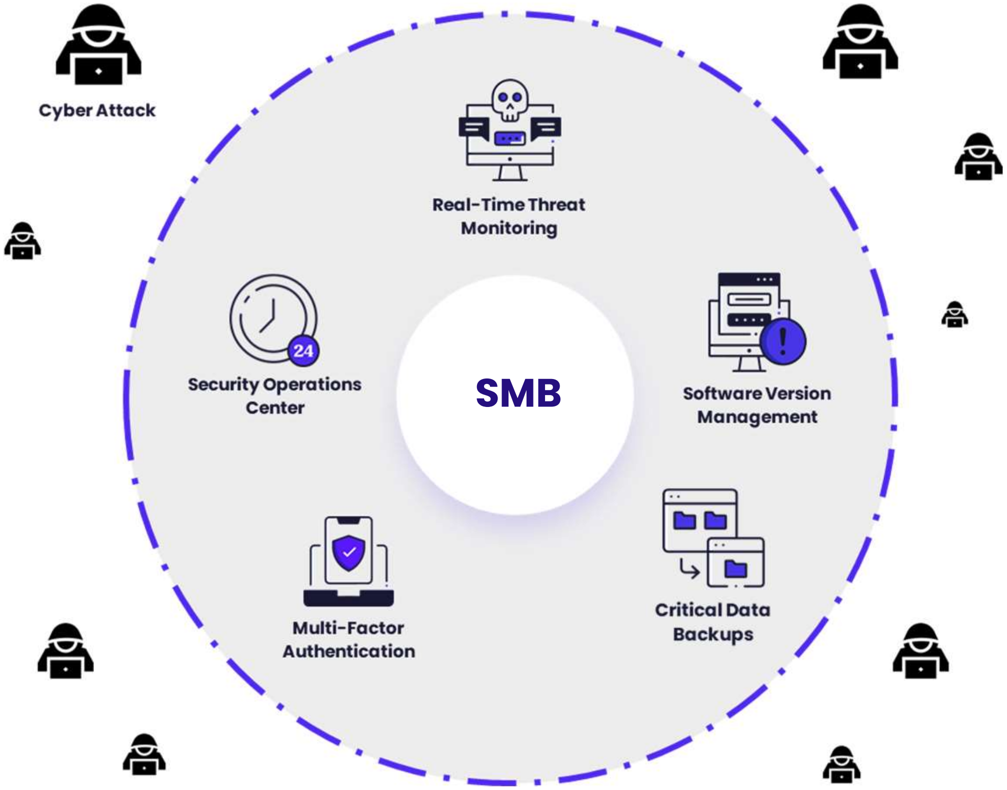
- Cyber Crime is real and the liability is massive. Unlike a slip and fall, an Employment Practice Liability (EPL) or Workers CoLS0claim, Ransomware can put an organization out of business.
- Cyber insurance and cyber security controls are no longer a luxury product. A proper security posture including backups, MFA, IR plans, endpoint security and patching is now mandatory.
- Commercial contracts increasingly stipulate cyber insurance be in place for any organization that maintains Personally Identifiable Information.

How can a small business possibly keep up with compliance, contractual obligations and afford their evolving cyber needs?

NCPA NATIONAL COMMUNITY PHARMACISTS ASSOCIATION

Best Practices for Preventing & Recovering from a Cyber Attack

- ✓Proper Controls in place
- ✓IR Plan & Team
- ✓Cyber Insurance Policy
- ✓Employee Training
- ✓Pen Testing



Cyber Attack

Real-Time Threat Monitoring

Security Operations Center

SMB

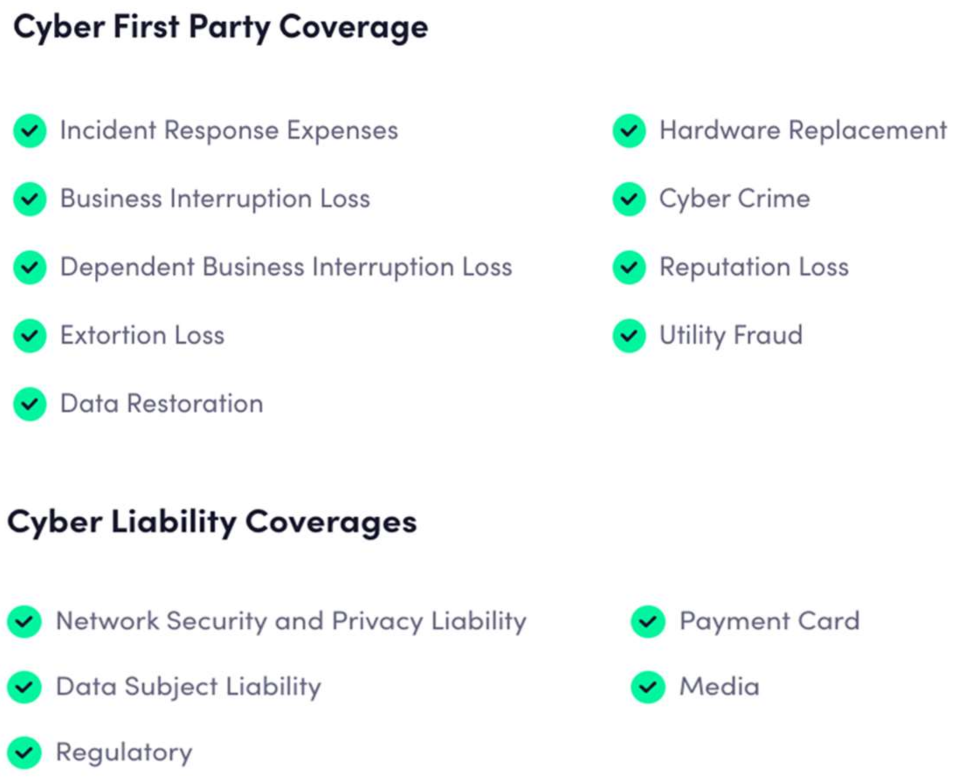
Software Version Management

Multi-Factor Authentication

Critical Data Backups

Coverage that can save the day

A cyber attack can happen to anyone. Cybersecurity controls although necessary, are not bulletproof. You must have a recovery plan which is why a Cyber Insurance Policy is imperative in 2024. What should it provide?



Cyber First Party Coverage

- ✓ Incident Response Expenses
- ✓ Business Interruption Loss
- ✓ Dependent Business Interruption Loss
- ✓ Extortion Loss
- ✓ Data Restoration
- ✓ Hardware Replacement
- ✓ Cyber Crime
- ✓ Reputation Loss
- ✓ Utility Fraud

Cyber Liability Coverages

- ✓ Network Security and Privacy Liability
- ✓ Data Subject Liability
- ✓ Regulatory
- ✓ Payment Card
- ✓ Media

Questions?

Contact Information

Justine Del Prete

Director of Sales and Marketing – Elpha Secure

Justine.delprete@elphasecure.com

Denise Ricardo

Cyber Program Manager, Bolton Street Programs