# CYBERSECURITY

JOHN WOODALL

3.02.23

# AGENDA

INTRODUCTION

PHISHING

RANSOMWARE

DATA BREACH

NETWORKS

IT SUPPORT

CLOSING

# INTRODUCTION

CYBERSECURITY

Who is this guy?

What is cybersecurity?

What do attacks and risks look like?

What can we do?

What do we need?


# PHISHING

DON'T GET HOOKED

# PHISHING DEFENSE

Why phishing?

What can you do?

Security Training for employees

MFA – Multifactor Authentication

Email Protection tools

SPF, DMARC, DKIM

Response

- Don’t click
- Use alternate, trusted source
- Delete

Got hooked?

- Write down details you provided
- Change passwords
- Notify IT
- Report to law enforcement if appropriate (ID/$)

# RANSOMWARE

DIGITAL BLACKMAIL

# RANSOMWARE




Colonial Pipeline Company

CNA

CITY OF DURHAM

# PREVENTION & RECOVERY

USER TRAINING

LOCK DOWN

LIMIT ACCESS

ANTIVIRUS/MTR

FIREWALL

BACKUPS

AIR-GAPPED

HISTORICAL

BARE METAL

CLOUDSIDE DATA

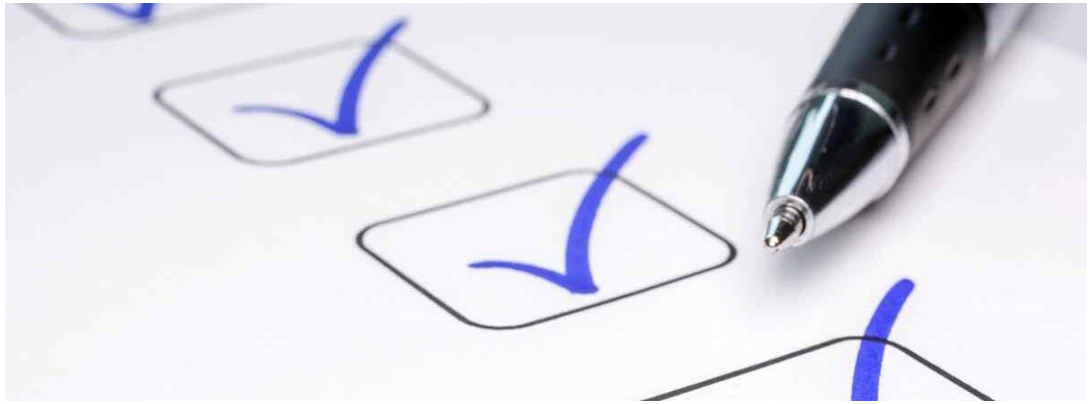
# PROTECT YOUR SENSITIVE DATA

MITIGATING RISK

# WHAT'S YOUR EXPOSURE?

| LOW | MODERATE | HIGH | INSANE |
| --- | --- | --- | --- |
| Employee work phone and email addresses. | Customer's name, address, credit card. | Employees' or customers' Social Security numbers or medical information. | Confidential corporate info, trade secrets, or government classified information |

# MANAGE RISK



## ENCRYPTION AT REST

- Sensitive information/fields
- Database
- Storage
- Mobile devices

## ENCRYPTION IN FLIGHT

- Local equipment, secured & segmented
- Secure Payment Processor
- P2PE – device level encryption
- Update firmware/software/protocols

# MITIGATION

## TRAINING

- PCI Compliance
- Identify PII/sensitive information
- POS devices, tampering
- Permitted maintenance

## ACCESS CONTROL

- Principle of Least Permissions
- Local Admin
- Convenience is the enemy of security
- Disable terminated users
- Avoid, but change shared passwords

## PASSWORD MANAGER

- Unique passwords
- Avoid weak passwords
- Business eyes on password strength
- Succession capability
- Safer sharing

# BREACH PREPARATION

## IDENTIFY A POINT PERSON

Clear understanding business's IT systems & data.  Quick thinking.

## CREATE A RESPONSE PLAN

Work with vendors.  Develop procedures for identifying, containing, reporting.

## TRAIN EMPLOYEES

Who is responsible for what?

## ESTABLISH COMMUNICATION CHANNELS

How are incidents reported? Consider other stakeholders

## CONDUCT REGULAR TESTING & UPDATES

Test regularly.  Update as needs and people change.

# BREACH RESPONSE

## IDENTIFY

Suspicious activity, reports

## CONTAIN

Take offline (leave on)

reset credentials

## NOTIFY KEY STAKEHOLDERS

Notify IT Support, payment processor, insurance, legal.

## INVESTIGATE

IT Support investigation.

Forensic skillset required.

## NOTIFY INDIVIDUALS

Employees & customers.

Type of data.

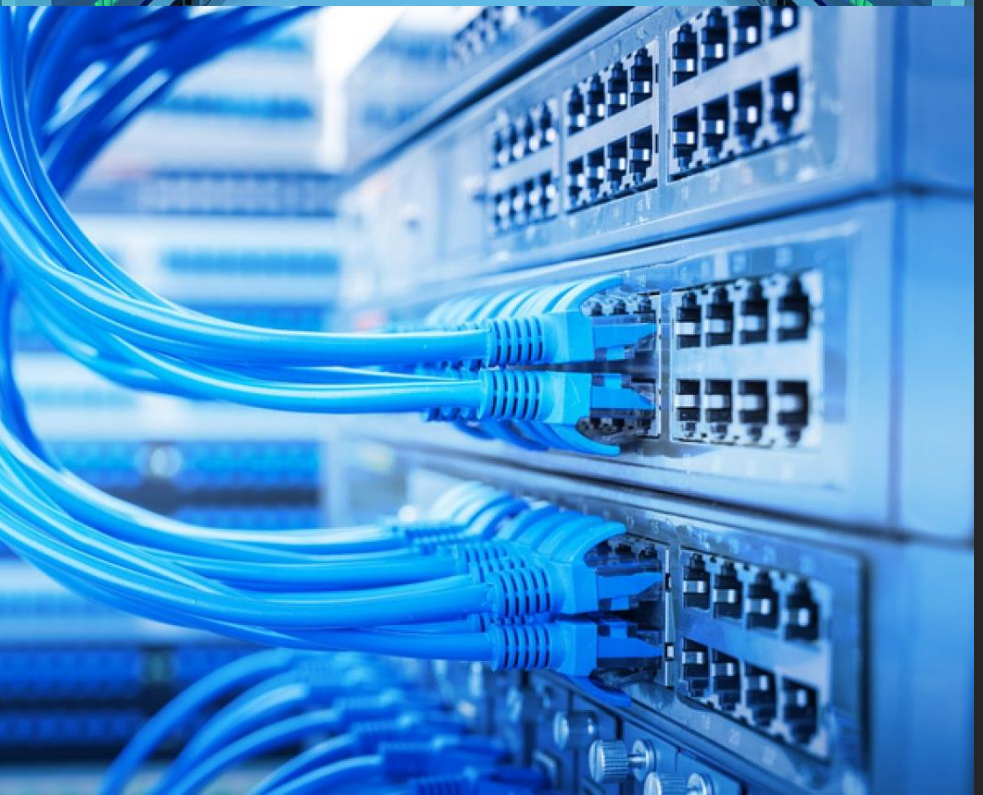
Next steps & guidance.

## REPORT BREACH

Regulatory authorities or local law enforcement as required.

## RESTORE SYTEMS

Notify IT Support, payment processor, insurance, legal.



# NETWORKING

BUSINESS CLASS, FOR A REASON

# HARDWARE AND SOFTWARE

## RISKS

Basic business functionality

Unhappy customers

## TECHNICAL DEBT

Computer upgrades

Software versions

Network equipment

## BUSINESS CLASS EQUIPMENT

Redundant Internet – SD-WAN

Advanced Firewall – High Availability

Switches - Managed, PoE

Wireless Access Points – Well designed

Network Health & Segmentation (VLAN)

– Corporate LAN, POS, Corp WiFi, Guest, HVAC, Security

Servers – Resilience, function segmentation, 5-6 years

Computers – Updates, protection, 3-4 years

UPS (Battery backup) – 3-5 years

# IT SUPPORT

MANAGED SERVICE PROVIDERS

# FIND YOUR IT TEAM

BUSINESS TENURE

TECH CERTIFICATIONS

PARTNERSHIPS

INDUSTRY EXPERIENCE

RESPONSE TIME/SLA

PROACTIVE VISITS

MONITORING

CONSULTING & PROJECTS

DISASTER PREPAREDNESS

CYBERSECURITY

IT BUDGET PLANNING

AUTOMATION & INTEGRATION

# IN CLOSING


CYBERSECURITY NETWORKS IT SUPPORT

# THANK YOU


JOHN WOODALL

(704) 361-3789

Jwoodall@

carmelcountryclub.org


HFTP CYBERSECURITY