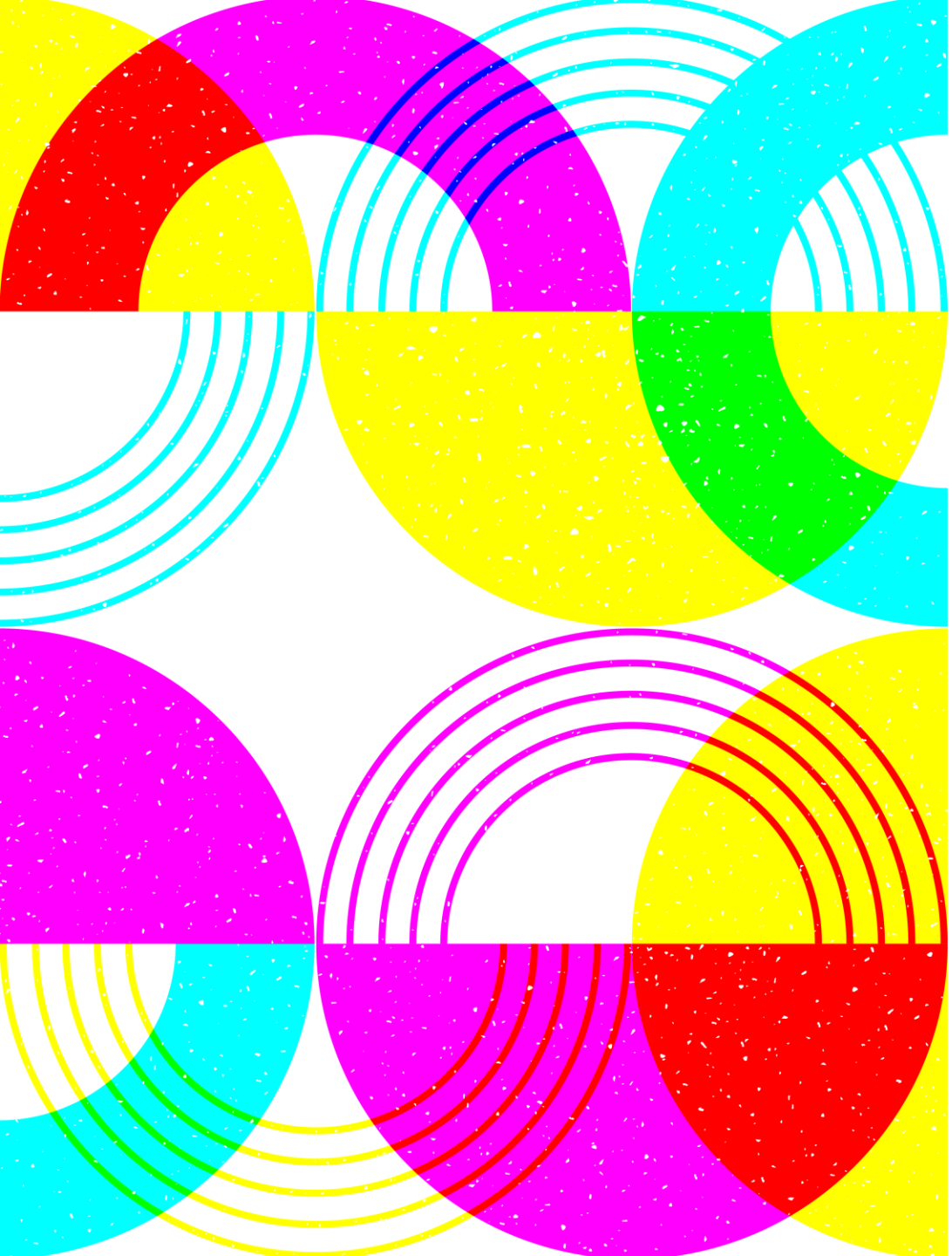


follow us on social!

#skyicon



SKYWARD®

iCON

Ransomware Readiness - Building Resilient IT Defenses

Mike Bianco – VP of Information Security

Ransomware Readiness - Building Resilient IT Defenses

- Before the Event
- During the Event
- After the Event

Why are you here?

Education is a prime target for ransomware attacks. In this session, you'll learn how to safeguard your district by implementing a comprehensive Security Awareness program for your users.

Best practices for database backups and rebuilding on-premises Skyward servers after a ransomware event.

Also conducting Security Assessments to ensure your network adheres to Security Best Practices and equip yourself with the knowledge to defend against ransomware and protect your district's valuable data.

Ransomware “Fun” Facts

- **K-12 schools remain one of the most targeted sectors**, with ransomware incidents rising sharply—U.S. educational institutions saw a 35% increase in attacks (217 total) in the most recent year studied, and 82% of K-12 organizations experienced cyber threat impacts across 2023–2025. [edscoop.com]

- **The financial and operational impact continues to worsen**, with average K-12 ransomware recovery costs reaching $2.28 million in 2024—the highest among major sectors—and attacks frequently disrupting learning, meal programs, counseling services, and exams. [cisecurity.org]

- **68% of all breaches involve the human element**, including errors, social engineering, misuse, and credential-related missteps (non-malicious human actions remain the dominant factor). [sophos.com]

- **97% of breaches in North America are financially motivated**, with external attackers still representing the overwhelming majority of threat actors.[eschoolnews.com]

- **Ransomware/extortion remains involved in ~32% of breaches**, holding steady as one of the top Action types across nearly every industry. [fdd.org]

Victims of Ransomware



Are you aware of a school, business or individual who has been a victim of ransomware?

Best Practices

- **Security Awareness Training**
  - Are you user's trained to be a human firewall?
- **Use the Principle of Least Privilege**
  - If the user that initiated the attack can't access the data, it can't be encrypted.
- **Endpoint Detection & Response (EDR)**
  - Ensure it is up-to-date and that end users cannot disable it.
  - EDR is more that just Anti-virus
- **Endpoint Patch Management**
  - Keep systems current with Operating System and software patches, including Skyward.
- **Remote Access**
  - If remote access is required, it must be secured using MFA.
- **External Attack Surface Management**
  - Ensure Firewall Intrusion Prevention is enabled detect/prevent attacks.
  - Ensure only necessary systems and ports are accessible to the internet.

BEFORE: User Awareness

Can your end users spot a phishing attempt?

- Using KnowBe4, initial baseline testing in education settings found that as much as 32.7% of users failed phish tests
- With a training program the failure rate can drop to as little as 4% after 1 year
- 7-10% of phish attempts will make it past your email filters
- Training needs to be consistent and continuous – don't settle for ten minutes at the opening in-service program in August



Phishing by Industry 2022 Benchmarking Report by KnowBe4

BEFORE: Security Awareness Training

The KnowBe4 Security Awareness Program WORKS

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



BEFORE: Security Awareness Training



Does your District have a Security Awareness Training program in place?

BEFORE: Cyber Insurance



Be ready for questions from insurance company about the District's policies and practices

- They may want to know….
  - Does your district have security training for all employees?
  - How are backups handled for ALL systems used by the district?

Know the insurance policy

- What does it cover?
- What will it pay for a restorable event?

BEFORE: Disaster Recovery Plan

1. Does the district have a plan for emergency situations?
   - Tornado
   - Fire
   - Flood

2. What about?
   - IT Hardware
   - IT Services
   - Ransomware



3. A proper plan needs to include all parties!
   - IT staff
   - District administration
   - Other staff – teachers, office personnel, buildings and grounds, maintenance, etc.

BEFORE: Backup, Backup, Backup



Backup Server Best Practices

- Veeam says “DO NOT PUT THE BACKUP SERVER ON THE DOMAIN!!!!”

Be aware of the backup system’s limitations with app aware backup

- Progress database or SQL database

3-2-1 Rule

- Three copies, two different types of media, one media OFFSITE

Test the backup restore process regularly!!

BEFORE: Security Audits / Testing



- Network scan
- Policy review
- Practices
- Penetration tests

DURING: Do What?

Disconnect the infected system(s)

- Disconnect the Internet
- Network (isolate or unplug/disconnect)
- Do not shut device off (preserves all evidence)

Contact Stakeholders

- Cyber Insurance, Authorities, Incident Response team, Public Relations

DURING: Do What?

Determine the scope of the infection

- Locate patient zero and identify the strain
- Perform Forensic Investigations

Evaluate your options

- Restore from backup? or….
  - Decrypt
  - Do nothing (unlikely)
  - Pay the ransom (last resort)
- Repair Systems based on Criticality

Restore or Pay ?

Was data exfiltrated?

- *What data and does this matter?*

Are my backups safe?

- *Were they offsite, how old are they?*

What does the cyber insurance cover?

- *Is there a limit to how much ransom your district will pay?*
- *Is it ethical to pay?*

❖ **If you restore….**

- *Consult with vendors for each product prior!!*

❖ **If you pay….**

- *Consult with a professional before attempting to decrypt!!*

AFTER: Infected Systems

- Do not simply restore the system from a bare metal backup.
- Rebuild the machine and restore the necessary data only after it is verified safe.



Lessons Learned

- How did the infection **get through** your defenses?
- Where did the protections **break down**?
- **Adjust** district training programs!
- **Re-evaluate** policies / plans.
  - Insurance policies
  - Disaster plans

Skyward's IT experts have the latest knowledge on industry trends and developments to help keep your network running smoothly.

NETWORK CONSULTING

- Resilient Wired Network Infrastructure
- Complete Wireless Network Solutions
- Virtual Server Design and Support
- Storage Area Network Solutions
- IP Telephony Solutions

SUPPLEMENTAL IT STAFFING

- Onsite and Remote IT Support
- Network Assurance Services

ASSESSMENT SERVICES

- Network / Security
- Disaster Recovery
- Secure Cloud Computing

SKYWARD OPTIMIZATION

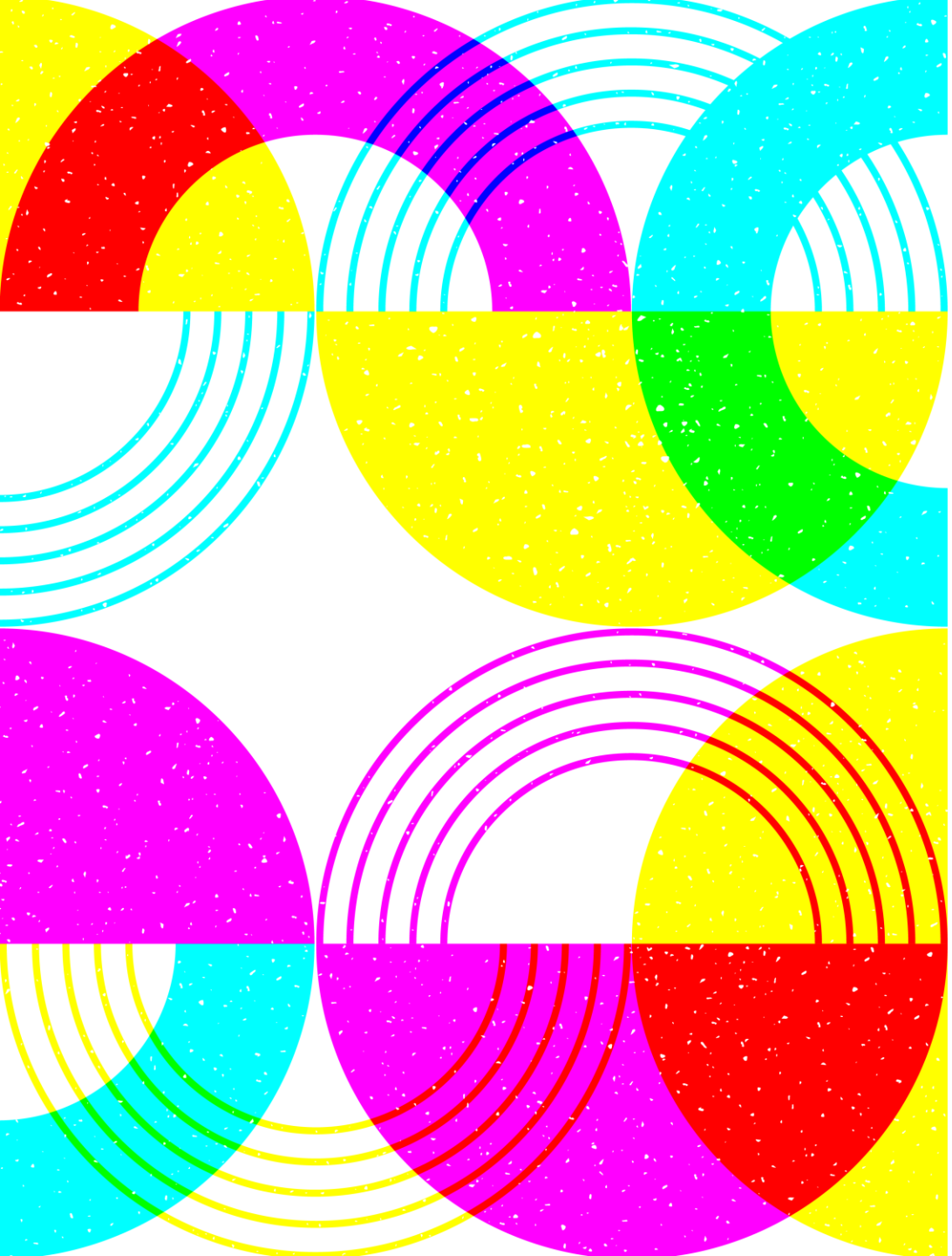
- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

NETWORK SECURITY SOLUTIONS

- Intrusion Detection, Prevention, and Next Generation Firewalls
- Email Filtering, Archiving, and Security Solutions
- Internet Filtering and Monitoring Solutions
- On-Staff Security Experts

DISASTER RECOVERY SERVICES

- Skyward Disaster Recovery from ISCorp
- Onsite Data Center Disaster Recovery Solutions



SKYWARD®

iCON

thank you!