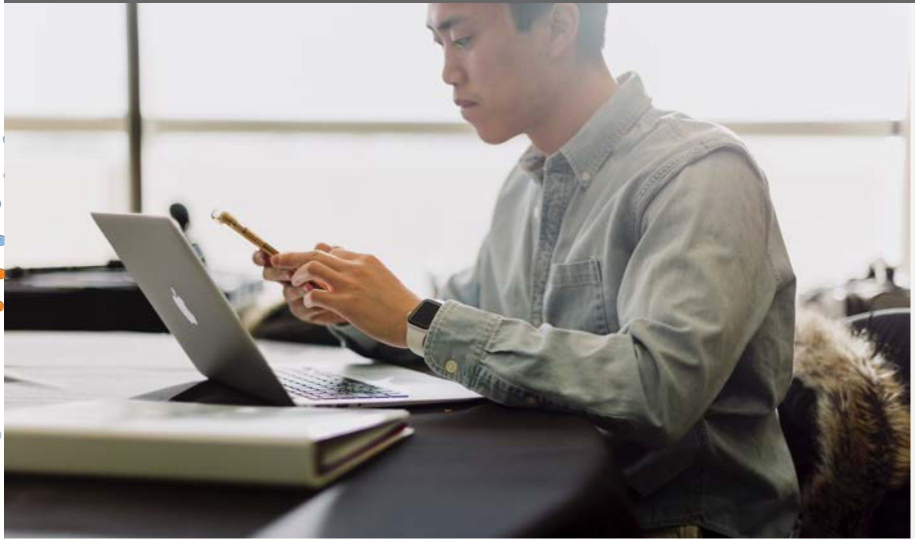
Nonprofit Cybersecurity Incident Report with Matthew Eshleman

Emerging Trends, Practical Advice



Community IT Innovators®

Where Technology Meets Mission

Learning Objectives

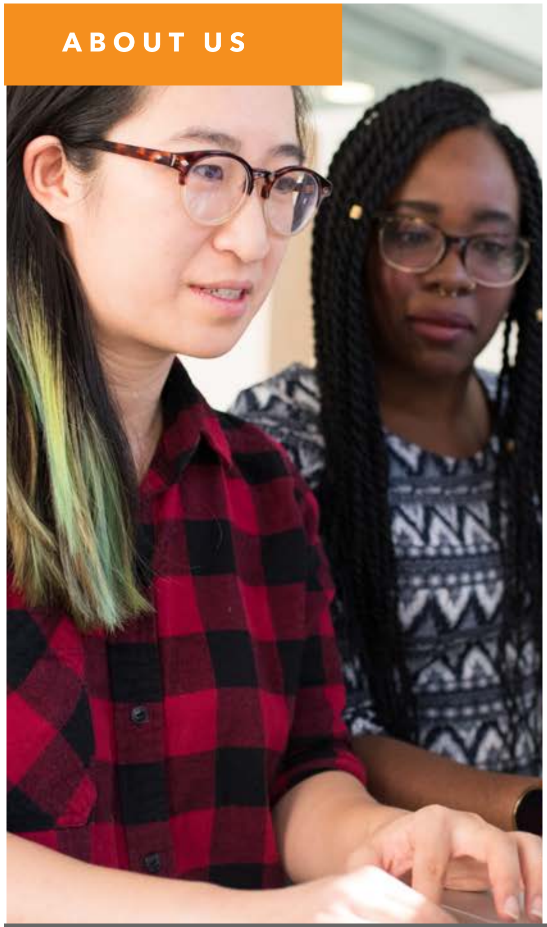
- Learn our basic approach to cybersecurity
- Learn the trends in attacks and organization protections we saw in 2023
- Understand evolving security best practices
- Learn the role of governance policies and training in protecting your nonprofit from common scams

PRESENTER

Matthew Eshleman

Chief Technology Officer
Community IT

ABOUT US



Advancing mission through the effective use of technology.

100% employee-owned

2023 WINNER

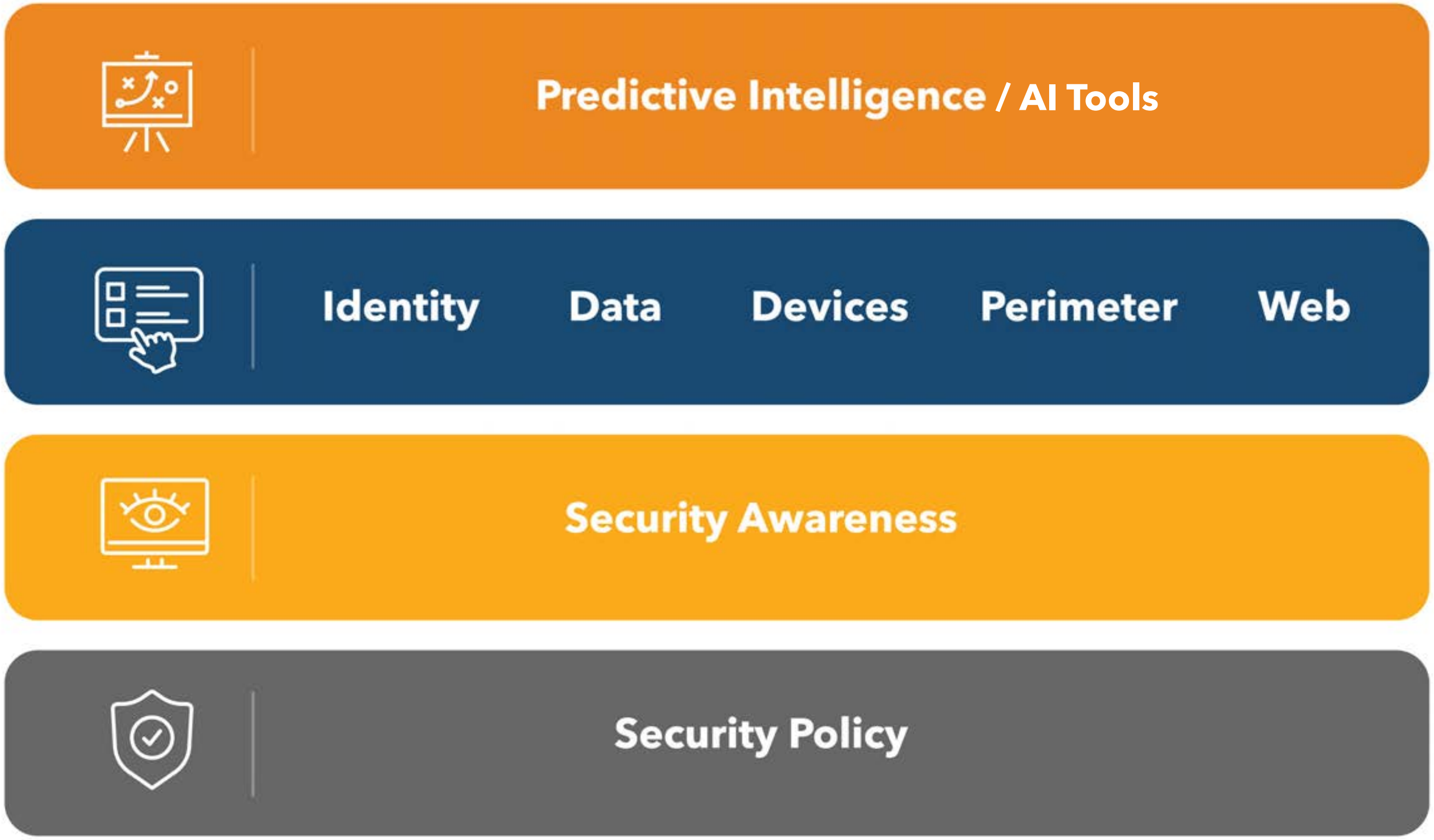
Channel Futures
Leading Channel Partners Forward
MSP 501

CommunityIT Innovators®

Poll 1: Has your organization had a cybersecurity incident in 2023?

1. No – Not that we know
2. Not sure
3. Yes, but we discovered it with time to mitigate the impact
4. Yes, and we suffered significant impact
5. Not applicable/Other

CommunityIT Innovators®



Predictive Intelligence / AI Tools

Identity Data Devices Perimeter Web

Security Awareness

Security Policy

Current Cybersecurity Landscape

- Cybersecurity impacts every organization
- Cyber criminals see their work as a job not a hobby
- Cyberliability insurance is normalizing strong controls and regular audits and updates to security
- Financial audits continue to impact IT
- Artificial Intelligence, the 2024 election, and other risks mean cybersecurity needs will continue to grow

Landscape: Hacker Approach

- Generic, automated attacks, viruses, malware are routinely blocked; nonprofits are at greater risk from more targeted scams and cons
- Compromise/spoofing/phishing still common
- Attacker-in-the-Middle (AitM) attacks new; compromising MFA-enabled accounts
- QR attacks new and more common
- In-person event/phishing scam is new

Landscape: Operation Trends

- Cyberliability insurance driving regular audits and stronger controls
- Artificial Intelligence (AI) is enabling new protections and also new scams and realistic cons
- Training and internal culture offer protection from wire fraud, phishing, other scams
- Data policies, AI policies, and Incident Response Plans are essential to organization operation

Definitions

- Multi-factor Authentication (MFA)
- Single Sign On (SSO)
- Credentials/Compromised Accounts
- Smishing
- Spear phishing
- Spoofing
- Ransomware
- Threat Actor
- Wire Fraud
- QR Code
- Malware Browser Pop-up

Poll 2: What kind of cybersecurity incident did you have in 2023?

1. None
2. Virus/Malware/Generic attack
3. Ransomware and a ransom was demanded and/or paid
4. Compromised account (credentials suspected or confirmed hacked)
5. Business Email Compromise (spoofing – your email was used to target others)
6. Advanced Persistent Threat (precise and targeted)
7. Wire fraud ($$ sent to hacker's account)
8. Other
9. Not Applicable

New Cybersecurity Attacks

- Phishing is more dangerous
- In-person event scam/phishing is new
- Pop-ups with virus warnings are new; viruses are still rare
- QR code scamming rising
- AI is enabling more realistic wire fraud attacks
- Smishing is increasing
- MFA enabled accounts can now be compromised by Attacker-in-the-Middle (AitM) attacks

CommunityIT Innovators®

Incident Report: Incident Count

HIGH RISK THREATS	
Brute Force Attacks	177
Compromised Account (confirmed)	44
Advanced Persistent Threat	8
Wire Fraud	5
Ransomware	0
Medium Risk Threats	
Compromised Account (suspected)	391
Business Email Compromise (or spoofing)	333
Low Risk Threats	
Spam	608
Malware	76
Virus	12
Grand Total	**1654**

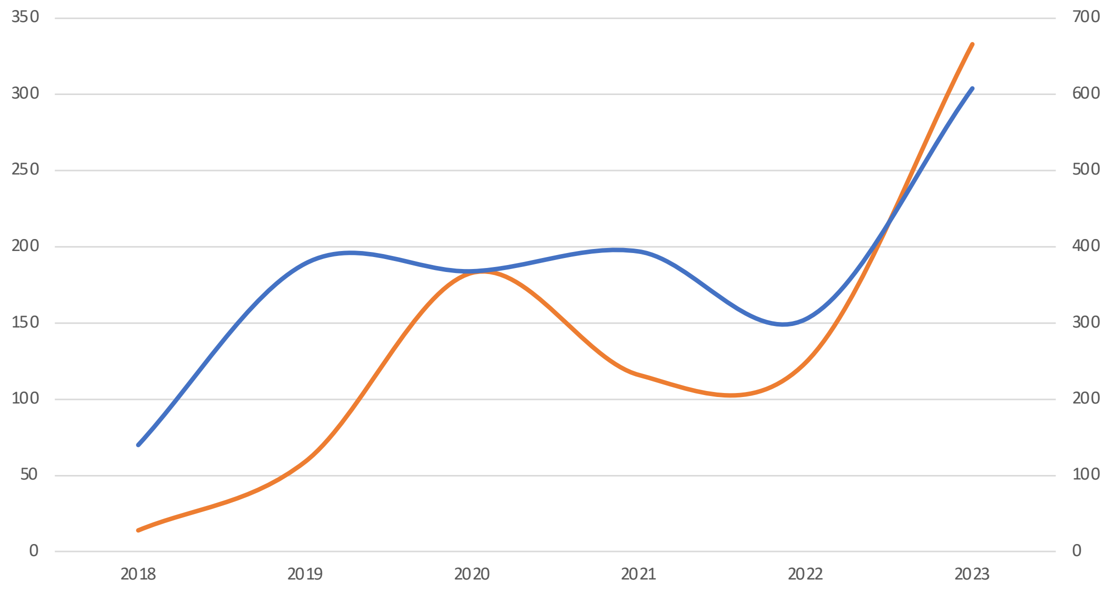
CommunityIT Innovators®

Incident Report: YoY Changes

Type	2018	2019	2020	2021	2022	2023	YoY 22-23
Spam	140	378	368	394	305	608	**99%**
BEC Spoofing Spear Phishing	14	59	183	116	124	333	**169%**
Malware	54	50	95	45	156	76	**-51%**
Virus	1	3	7	7	4	12	**200%**
Ransomware	0	0	1	2	0	0	
Account Compromise (Confirmed)	20	15	32	32	17	44	**159%**
Account Compromise (Suspected)				88	254	391	**54%**
Advanced Persistent Threat	1	1	4	9	12	8	**-33%**
Wire fraud	3	3	0	3	8	6	**-25%**
Brute Force Attacks			43	64	60	177	**195%**
Supply Chain	0	0	0	0	0	0	
Total	**233**	**509**	**690**	**696**	**940**	**1655**	**76%**

CommunityIT Innovators®

Incident Report: Spam & BEC



Incident Report: Trends in 2023

- Almost every type of attack is increasing
- Spam – it’s annoying but not too dangerous
- Phishing increasing – and it’s more dangerous
- In-person phishing is new
- Smishing increasing

Incident Report: Trends in 2023

- Pop-ups with virus warnings are new; viruses are still rare
- Wire fraud is rare but has major impacts
- QR code scamming rising
- MFA enabled accounts can now be compromised by Attacker-in-the-Middle (AitM) attacks

Protect Your Organization

- Review or establish governance policies on:
  - IT Acceptable Use
  - Incident Response
  - AI Acceptable Use
  - Disaster Response Plan
- Implement security awareness training against:
  - Email Phishing
  - Account Compromise
  - Wire Fraud
  - Business Email Compromise
- Update and upgrade MFA:
  - Protect Against Attacker-in-the-Middle Attacks
  - Use Phish Resistant MFA

Community IT Cyber Offerings

- Free initial assessment and discussion
- Free online resources
- NIST Security Survey
- In-Depth Cybersecurity Assessment
- Managed Cybersecurity Services
- Managed Cybersecurity Training for Staff

Q&A

Book time with Matthew Eshleman:
https://meetings.hubspot.com/meshleman

Thank You

CommunityIT Innovators®

Where
Technology
Meets Mission