



MSBO Annual Conference

Cybersecurity – A School's Journey





Ramifications



Covered

- › Cyber forensics
- › Legal
- › Notification costs (call center, credit monitoring, etc.)
- › Public relations
- › Data recovery
- › Ransom payments
- › Resulting lawsuits

Not Covered

- › Downtime
- › Disruption
- › Community relations
- › Staff relations
- › Reputational damage



Contact



- **Paul Grienke**
Sales and Development Specialist
pgrienke@setseg.org
517-816-1676

Who Is SET SEG?

The risk management experts providing solutions to help meet the unique needs of Michigan public schools



Property/Casualty Pool

530+ members

\$170 million in net
asset returns

Provides: property,
liability, auto, school
violent acts,
cyber protection



Workers' Compensation Fund

520+ members

\$301 million in
contribution
reductions

\$550,000 in Safety
Program returns



Employee Benefits

Healthcare, dental,
vision, long-term
disability

Consulting, compliance,
and administration
services



SET SEG Foundation

\$710,000+ in student
scholarships and grants

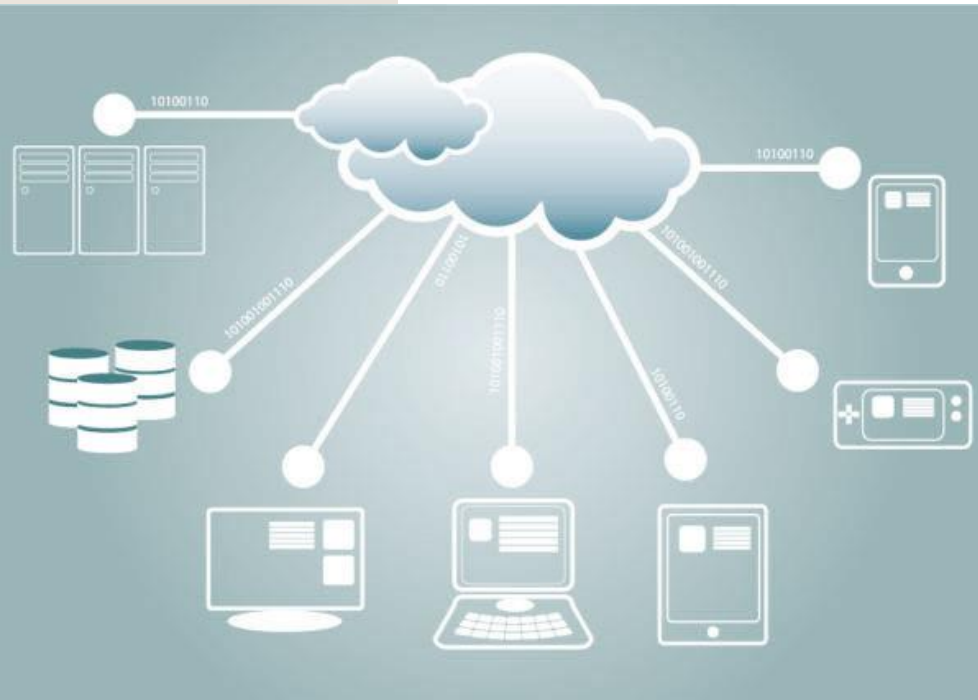
Promotes opportunities
in student leadership,
expanding educational
programs, skilled
trades, and risk
management studies





Cyber Risk

Why is this topic so important?



- › Reliance on technology
 - › HVAC, phones, security, etc.
- › Complex technology infrastructures
- › Remote learning
- › Massive amounts of data
- › Strained resources, funding, and staff



Why So Challenging?



ANN ARBOR

‘Data-rich, resource-poor.’ Why Michigan schools can be a ‘soft target’ for ransomware attacks

Updated: Mar. 06, 2023, 2:44 p.m. | Published: Nov. 20, 2022, 6:30 a.m.

Current State of Cybersecurity

LOCAL

Lansing Community College suspends most classes for 'ongoing cybersecurity incident'



Ken Palmer

Lansing State Journal

Published 6:32 p.m. ET March 15, 2023 | Updated 4:05 p.m. ET March 16, 2023



As hackers increase ransomware attacks, Michigan schools try to respond

Michigan Radio | By **Doug Tribou**, **Lauren Talley**

Published January 31, 2023 at 12:26 PM EST



▶ LISTEN • 6:40

University of Michigan shuts down school's internet connections following 'significant' cybersecurity incident



By **Sean Lyngaas**, CNN

2 minute read · Updated 7:46 PM EDT, Tue August 29, 2023



Raymond Boyd/Michael Ochs Archives/Getty Images/File

The Incident

- Overview
 - Experienced tech staff
 - 20+ years of experience
- November – The Call
 - Systems compromised
 - 125 servers
 - Downtime - 3 instructional days
 - Ransomware
 - \$700,000
- Immediate Response
 - Every second counts
 - Act swiftly and shut everything down
 - IT admin authority



Understanding Cyber Incidents

- Nature of the Threat
 - Feels like a home invasion
 - Intruder still in your home
 - Treat it like a crime scene
- Communication
 - Cautious communication
 - Alternative communication plans
 - Bad news travels fast



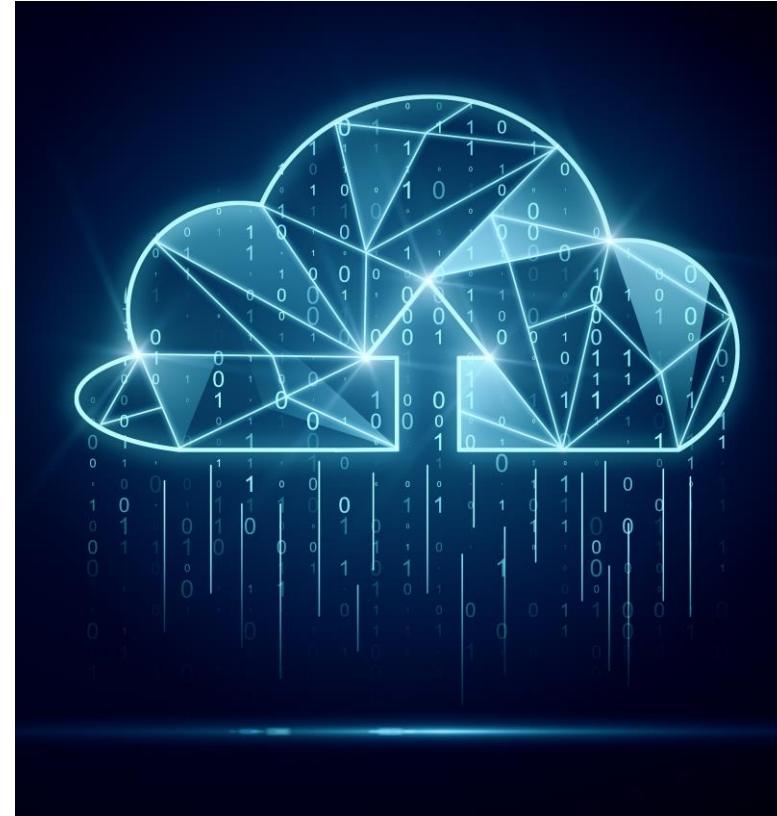
Steps in a Cyber Incident —

- First Call
 - Cyber insurance provider
 - We have the experts to help
 - Have emergency phone numbers ready
 - MSP – Cyber Command Center
 - FBI
- Steps to Take During a Breach
 - Refer to your written plan
 - Set up a command center
 - Insulate your tech team
 - Communicate to stakeholders
 - Food
 - Staff health



Challenges of Recovery

- Restoring From Backups
 - Restoration can be time-consuming
 - Average downtime – 10 days
 - Backups are not the solution to cyber breaches/incidents
- Policy Review and Updates
 - Regular review of your written plan(s) is crucial
 - Incident response plan
 - Business continuity plan



Experience and Lessons From the District

- Initial Ransomware Interaction
 - Extortion group – friendly and helpful
 - Don't open the ransom!
- Key Measurers Adopted
 - Managed detection and response – continuous monitoring for vulnerabilities
 - Endpoint detection response – protect their devices



Post-Incident Changes

- Infrastructure and Policy Enhancements
 - MFA mandatory
 - Comprehensive password management
 - Geofencing and disabling macros
- Organizational Changes
 - Increased security training and awareness
 - Hired dedicated cybersecurity personnel



New Reality – Post-Breach

- Operational Impacts
 - Increased operational costs and restrictions
 - Stringent control measures
 - Less convenience
- Continued Vigilance
 - Maintain robust security measures
 - Be prepared for repeat attacks



Impact to Schools

Attack Vectors

- Email phishing
- Clicked on malicious link
- Social engineering
- Gaining student credentials
- Monitoring and access open RDP port

Issues

- Secondary attack – manage breach yourself
- Wire transferring money to fraudulent vendor
- Servers, workstations and backups non operable
- Disruption and loss of student data

Reminders

- Timely reporting
- Phishing Training
- Use VPN/MFA
- Have & follow business office process
- Backups segregated and tested
- Network segmented/ EDR detection

Results

- Ransom demand increase with more systems locked up or secondary attack
- Wire transfers can be risky
- Higher deductibles upon renewal
- Time and reputational damage

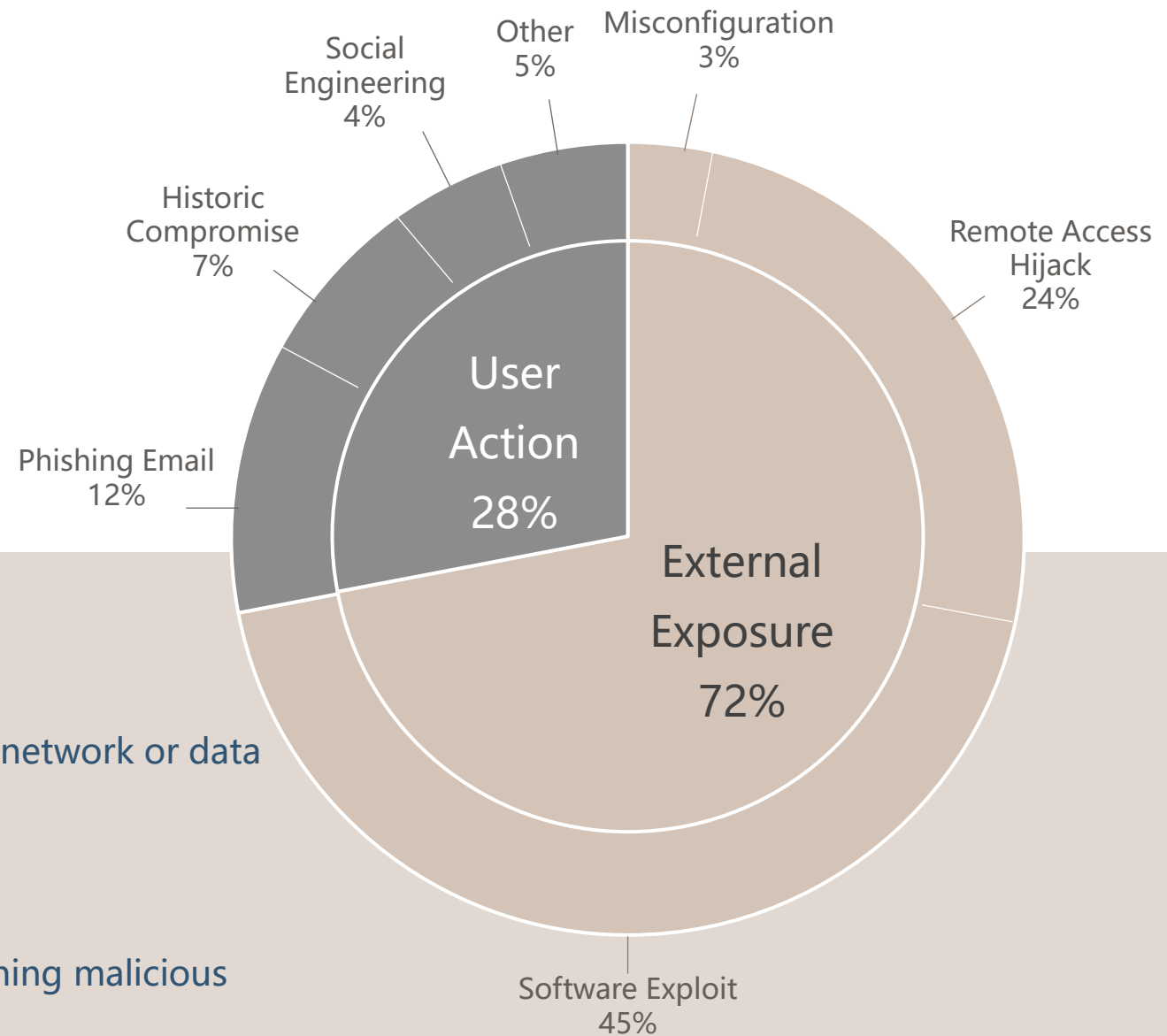
Organizations of different types, sizes, and budgets have had breaches:
K-12 w/ enrollments of 1,200-10,000+
ISDs w/ annual revenue of \$20M-\$170M

Root Point of Compromise

The root point of compromise (RPOC) is the initial entry point or a threat actor – how they gained initial access to a victim

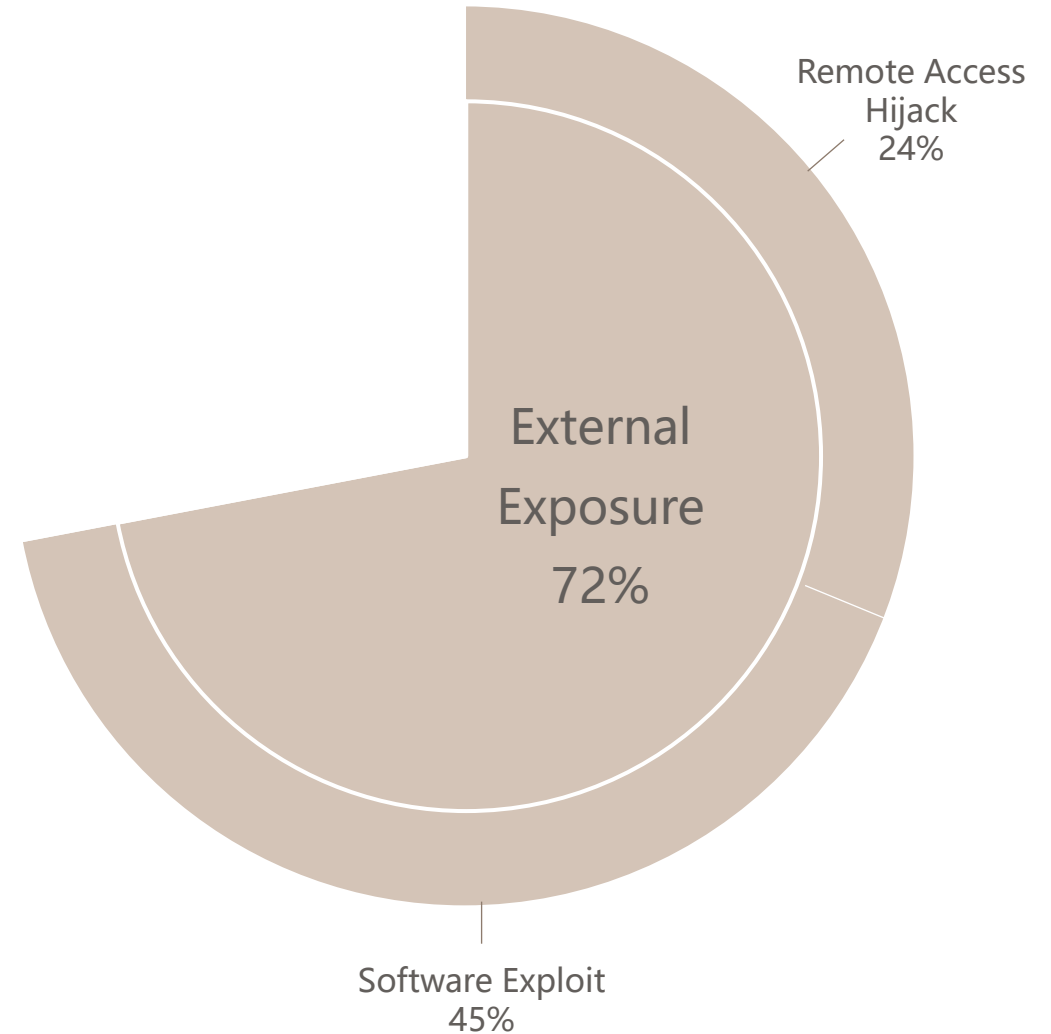
RPOC can be categorized in two ways:

- External Exposure
 - Attacker targets a victim and gains access to the network or data
 - Easiest method, widely used
- User Action
 - Attacker gains access due to a user's action (opening malicious files, re-using passwords, social engineering)

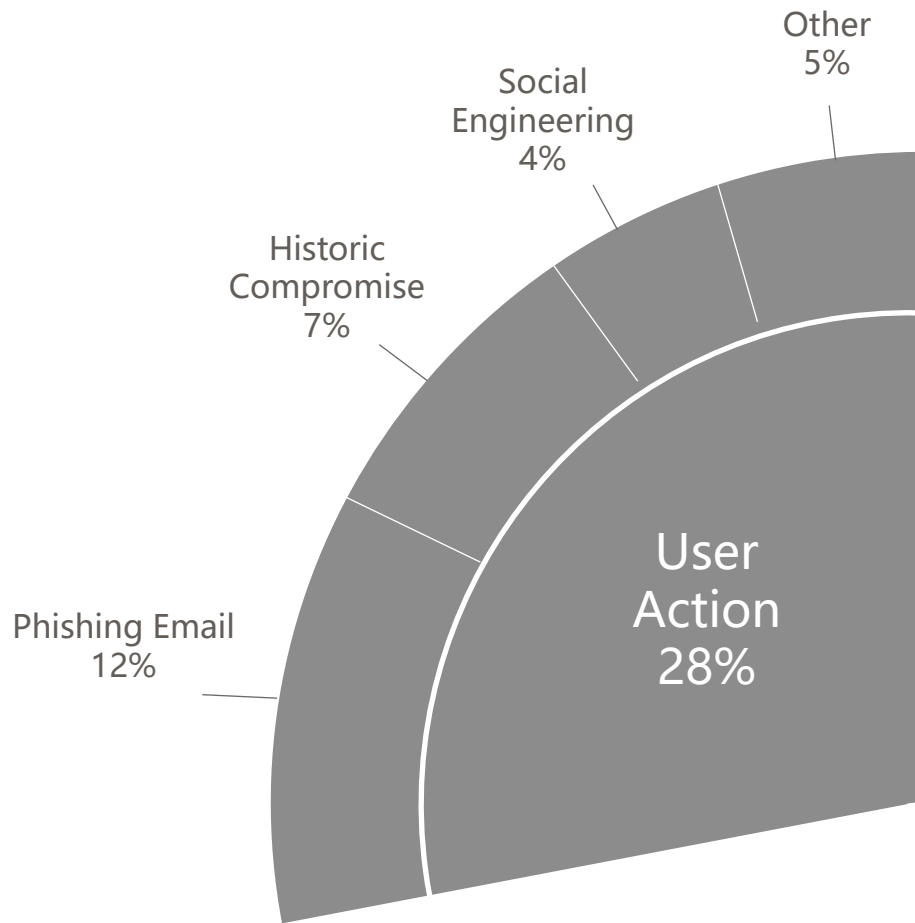


External Exposure

- > Software Exploit
 - > 45% of incidents caused by vulnerabilities that could have been mitigated through security updates
- > Remote Access Hijack
 - > 24% of incidents caused by IT practices that allowed remote access from outside the network
- > Misconfiguration
 - > 3% of incidents caused by misconfigurations of IT systems



User Action



- > Phishing email
 - > An email containing malicious links or attachments
- > Historic compromise
 - > Attackers had credentials from previous breaches and used them to access accounts
- > Social engineering
 - > Scam phone calls (vishing), text messages (smishing), and other deceptive means
- > Other
 - > Mistakenly downloading malicious, spoofed software in "drive-by" attacks
- > IT teams can thwart these attacks with email filters, security training, etc.

The Process of a Ransomware Claim

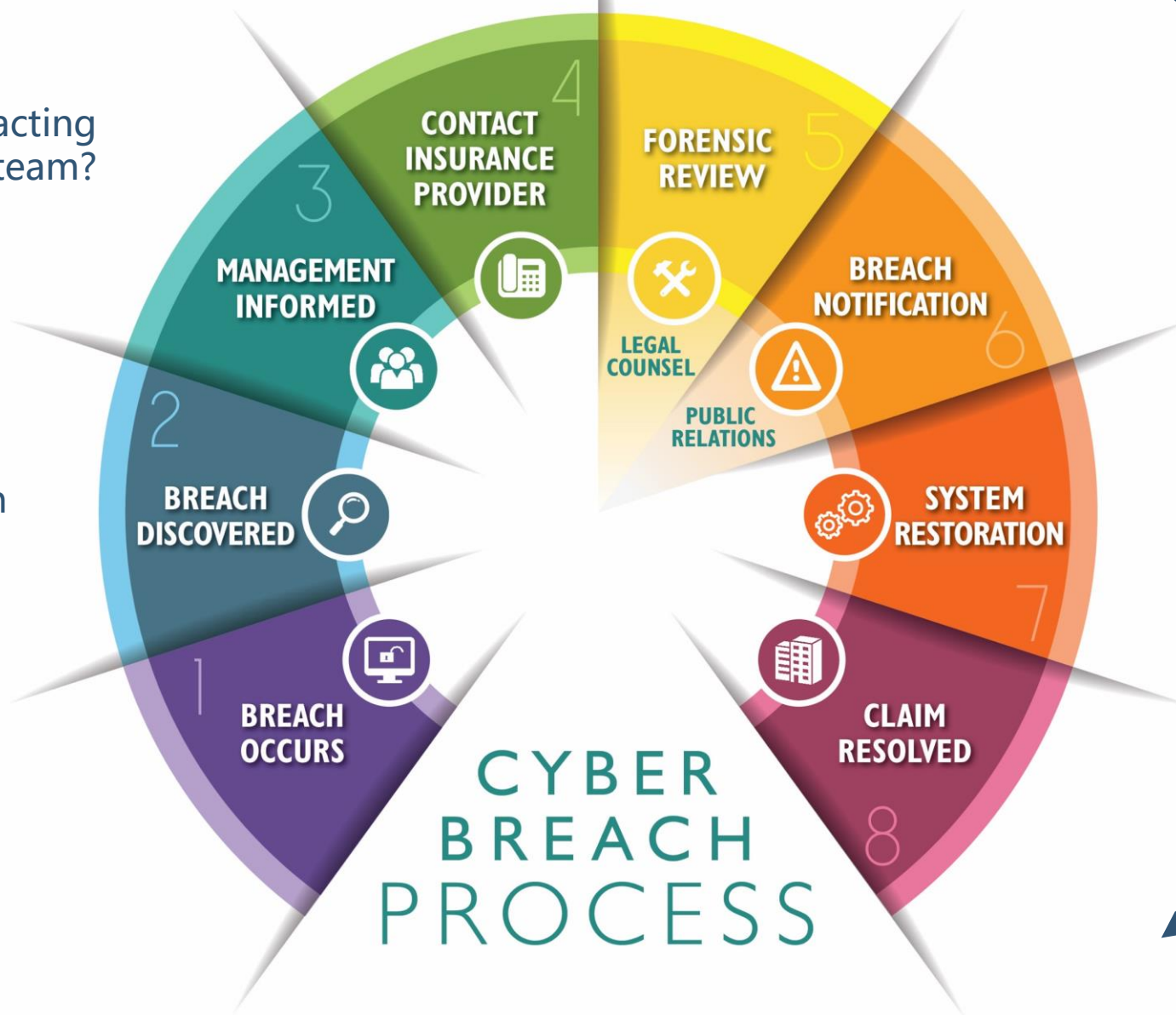


Incident Response Plan

Who are you contacting within your team?

Do you have your insurer's contact info ready?

Let the cyber mitigation specialists take over



Ransomware Guide



ARCTIC WOLF Incident Response



DON'T PANIC!

Try to remain calm and rely on your preparations and team to proceed.



REFER TO YOUR INCIDENT RESPONSE PLAN

The plan holds valuable information you and your IT team need if you are experiencing a security incident. Be sure the IR plan is updated frequently and printed out on paper.



REACH OUT TO YOUR TRUSTED ADVISORS

Insurance brokers, insurance claims team, legal counsel, etc.



ISOLATE YOUR BACKUPS

Ensure that your fire engine is far away enough from the fire in effort to save the burning house.



DISCONNECT SERVERS AND CRITICAL DEVICES FROM THE INTERNET AND EACH OTHER

If an attacker is taking data from your network in real-time, cutting off the internet will kill this action.



Our top ten tips to
mitigate an active
ransomware attack
in partnership with



GO BEYOND the typical IR experience



DO NOT ENGAGE THE THREAT ACTOR

Do not attempt to negotiate with threat actors or decrypt ransomed data on your own. Contact Arctic Wolf to save time, money, and your data.



DOCUMENT WHAT YOU CAN (SCREENSHOTS, PHOTOS, ETC.)

- Ransom notes / file extensions
- Reviewed logs
- Software conveying the state of the environment



PRESERVE ALL EVIDENCE

- Do not turn off devices
- Do not wipe/re-image/restore from backup without consultation
- Failure to preserve all evidence will result in an incomplete investigation



CHANGE YOUR PASSWORDS & ENFORCE MULTI-FACTOR AUTHENTICATION

- Administrator accounts / all cloud accounts
- VPN / remote connectivity software
- Firewall
- Email



IDENTIFY WHERE SENSITIVE INFORMATION IS STORED

Know the host name of this device, review your backups for this information. Consult with your legal team before you inform employees, clients, etc. of the attack.

©2023 Arctic Wolf Networks, Inc. All rights reserved.



ABOUT Arctic Wolf Incident Response

Arctic Wolf Incident Response is a trusted leader in incident response that enables rapid remediation to any cyber emergency at scale. Valued for breadth of IR capabilities, technical depth of incident investigators, and exceptional service provided throughout IR engagements, Arctic Wolf Incident Response is a preferred partner of cyber insurance carriers.

In partnership with





Technology



- Multifactor authentication (MFA)
- Offline, encrypted backups
- Phishing training for staff
- Business office training for verifying requests
- Engage experts immediately



Resources





Cybersecurity for Educators – How to Become a Human Firewall

Course #01

- Passwords, Phishing, MFA, ...
- 1 SCECH credit
- FREE

Course #02

- PII, Sharing Data Securely, Recognize, Respond and Report
- .75 SCECH credits
- FREE



SafeSchools



ESSENTIAL CYBERSECURITY PRACTICES FOR K12

Produced by METL (Michigan Education Technology Leaders), a MAISA affiliated Organization.
Created for Michigan schools,
by Michigan technology experts.



FOR MORE INFORMATION | www.misecure.org



merit

KnowBe4
Human error. Conquered.



Improve Insurability

JumpStart Threat Scanner

SCAN RESULTS:
Last Scanned: 02/02/22 | 51 Threats Scanned | 4 Locations ✓ | 2 Issues Found

Active Vulnerabilities:

⚠️	Microsoft Exchange Server Vulnerability CVE-2020-0796	Date Found 10/10/22	Domains 2	⬆️
----	---	------------------------	--------------	----

Description:
A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

[Get Help](#)

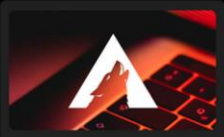
Previous Vulnerabilities:

✅	Citrix Vuln CVE-2020-0796	Date Resolved 10/08/22	Domains 3	⬇️
---	-------------------------------------	---------------------------	--------------	----

Scanned Vulnerabilities:

[View All](#) | Last Updated: 11/01/22 | Vulnerabilities: 51

Vulnerability Name:	CVE Number:	Date Added:	
VMware Horizon - "Log4j"	2020-44228	10/10/22	🔗
Microsoft Exchange Server	2020-34473	10/10/22	🔗
WSO2 Products	2020-29464	10/10/22	🔗



Let Arctic Wolf Help!

[Get In Touch](#)

THE LEADER IN **SECURITY OPERATIONS**

IDENTIFY

Our prioritized approach allows you to clearly see, remediate, and understand the most current and active threats that are present in your network.

Backed by Arctic Wolf Labs threat intelligence, Incident Response investigations, trillions of datapoints aggregated weekly across 4000+ client environments, and best-in-class 3rd party data sources, you can confidently find and fix the most severe threats first.

REMEDiate

Neutralize imminent threats in your network with our guidance through education, resources, or additional assistance from the Arctic Wolf team.

CONNECT TO EXPERTS

Seamlessly connect to the Arctic Wolf team and trusted partner network for any additional assistance in implementing security controls.

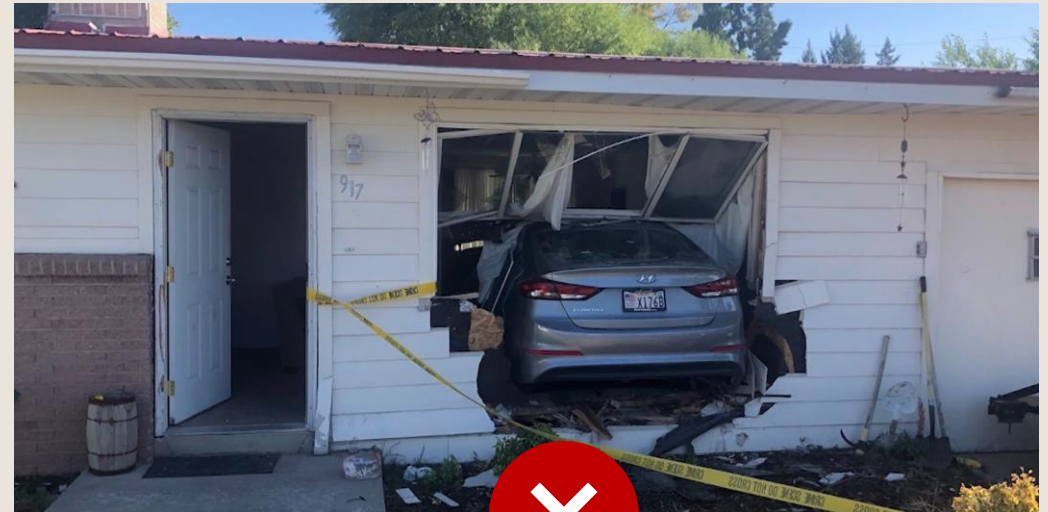
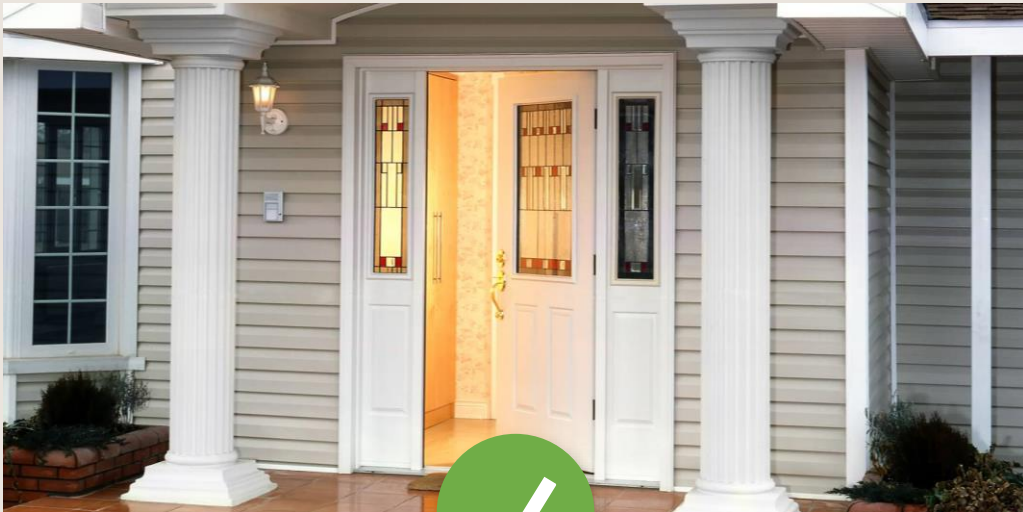


Arctic Wolf

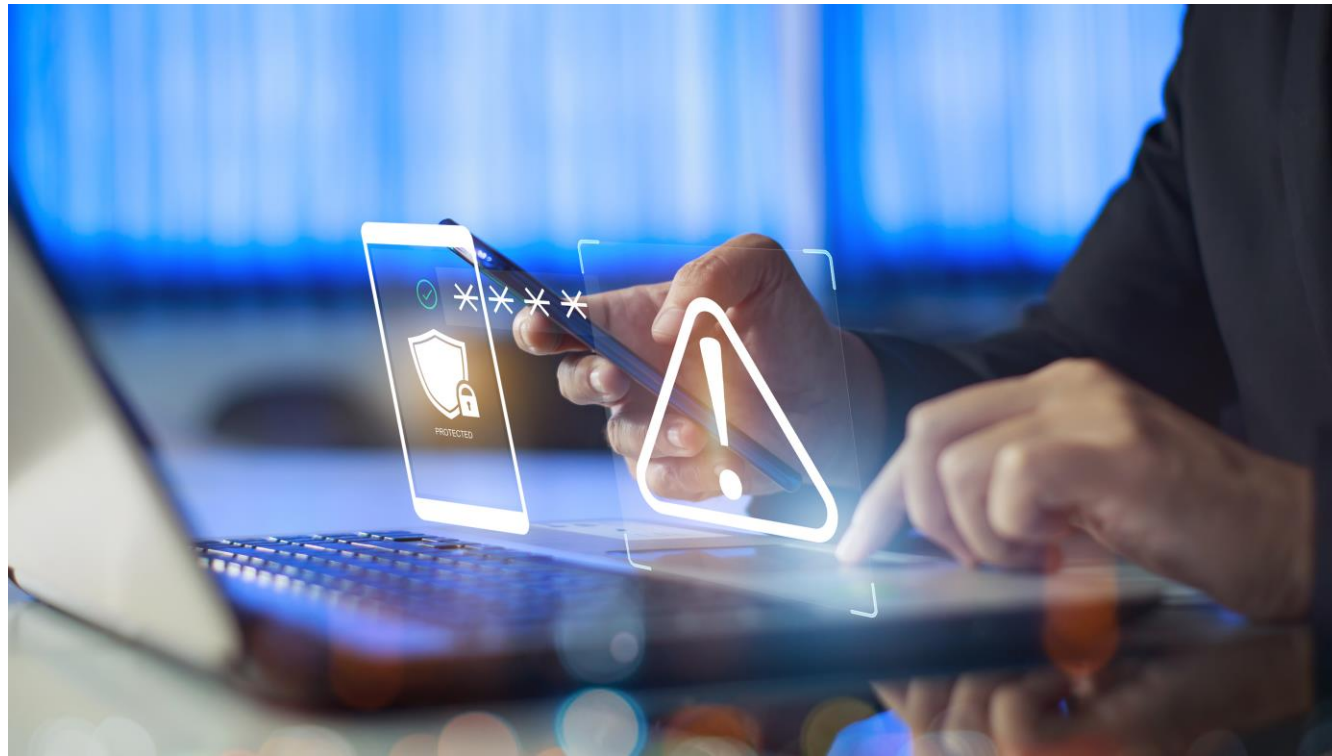
Cyber JumpStart Platform



External vulnerability scans are ...



Cyber Security Landscape







What Is _____ Cyber Insurance?



Cyber Insurance Changes?

- Renewals
 - Application process more challenging
- Lower Limits
 - Creating sublimit on amount of coverage
- Extortion/Ransom
 - Coverage may cease to exist in the future



Cyber Insurance Changes?

- Limited Market
 - Less appetite in the marketplace – will drive increased costs
- Increase Deductibles
 - Substantial increase in the marketplace
- Coinsurance
 - District paying for portion of claim cost
- Vulnerability Testing
 - Testing to conduct risk analysis





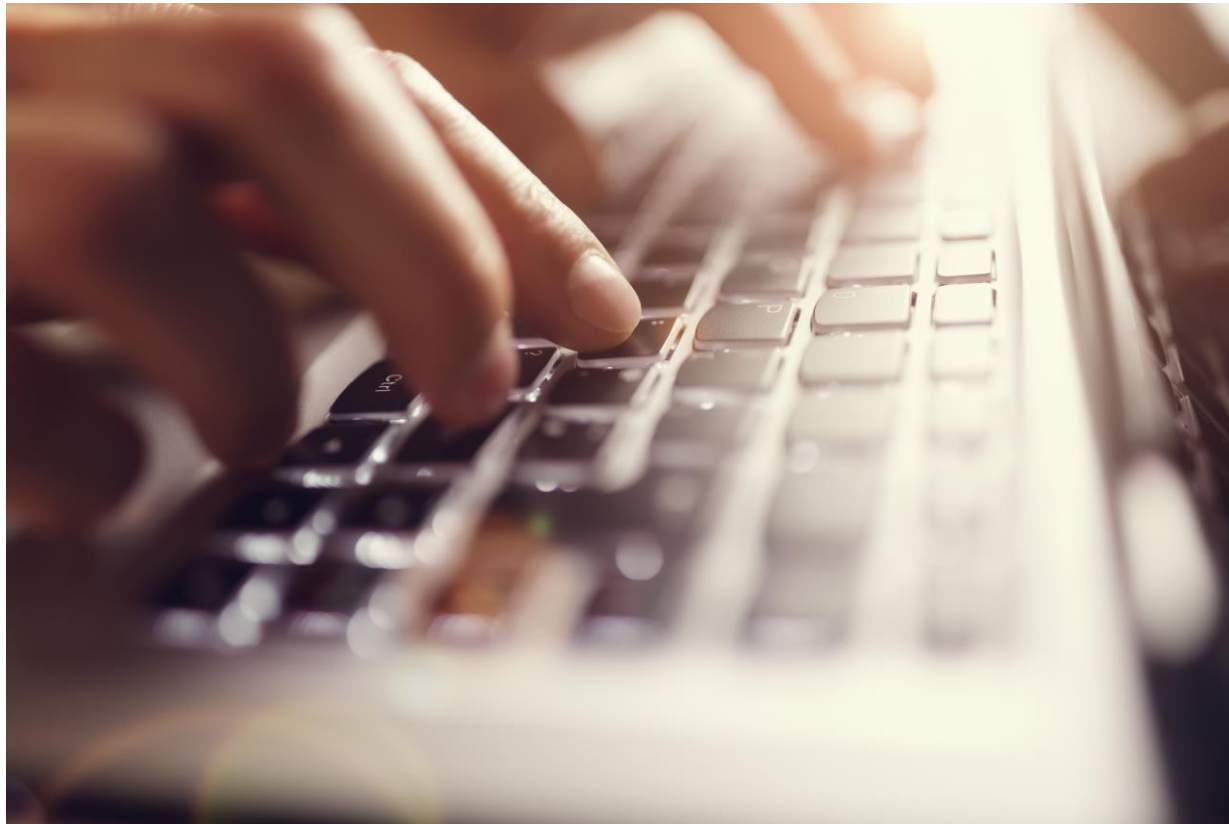
Future Requirements

From the Insurance Industry

- Phishing training
- Multifactor authentication (MFA) – remote access/critical information
- Backups offline/inaccessible to outsiders/encrypted/regularly scheduled
- Endpoint protection and response (EDR) and/or managed detection and response (MDR)
- Limiting administrative access
- System security patches updated
- Close open ports
- **Vulnerability scans are coming...**



Financial Impact



— The Cost

The impact of a breach extends beyond insurance costs



Relations

- Staff engagement
- Community frustration (paying ransom)



Insured Costs

- Deductible
- Premium



Disruption

- Downtime can be days to weeks
- Cancelled school
- Reconstruction of data



Non-Insured Costs

- IT security upgrades
- Employee wages (except overtime)
- Legal expense for updating cyber policies
- If ransom exceeds limit

Insurer Requirements

Deductible correlates to security

- No MFA for email
- No MFA for privileged users
- No EDR
- No advanced threat protection – O365
- End of life not segregated
- Users have local administrative rights
- No phishing tests
- No SOC
- No vulnerability scans
- Ad-hoc patching cadence





Questions?





Thank You!

