SET
SEG

CYBER SECURITY OVERVIEW

Who is SET SEG?

Property/Casualty Pool

- 530+ members
- $161 Million in net asset returns
- Provides: Property, Liability, Auto, School Violent Acts, Cyber protection

Worker's Compensation Fund

- 520+ members
- $301 Million in contribution reductions
- $550,000 in Safety Program returns

Employee Benefits

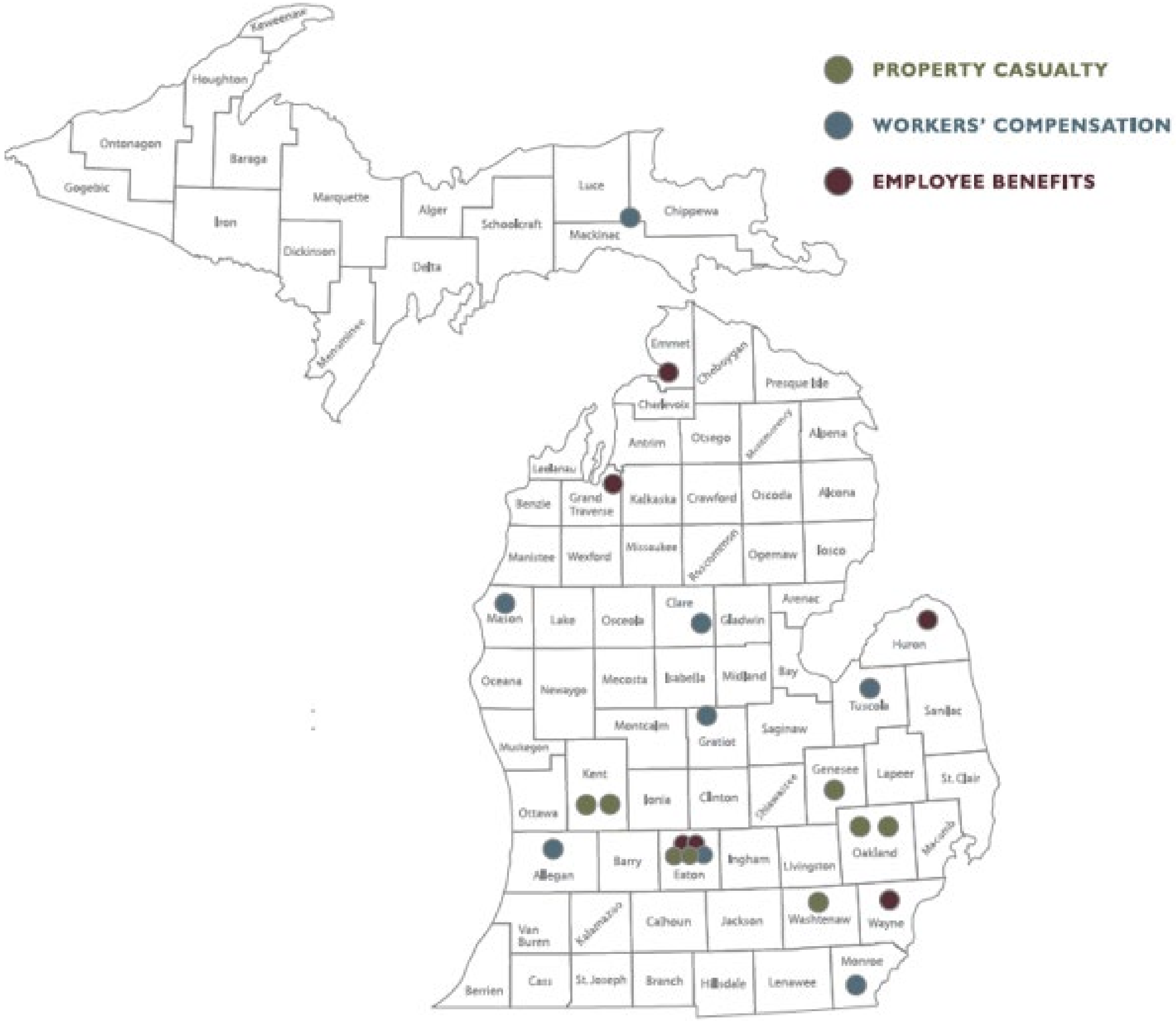
- Healthcare, Dental, Vision and Long-Term Disability
- Consulting, compliance and administration services

SET SEG Foundation

- $500,000 in student scholarships and Education Excellence grants
- Promotes opportunities in student leadership, skilled trades, and risk management studies

Governance & Service

The SET SEG programs are governed by over 35 superintendents representing districts of every size and type in every region across the state so that your voice and needs are represented at the table and decisions are made with your best interest.



Why Is This Topic Important?

5 Years Ago

- Smaller, unsophisticated attacks against public entities

Today's Environment

- Push to remote learning exposed vulnerabilities
- Heavy reliance on virtual learning / remote work
- Attackers want Personally Identifiable Information (PII) of students
- Attackers want to disrupt governmental entities
- Limited budget with complex IT environment

Ramifications

What’s Insured:

Cyber Forensics

Legal

Notification Costs
(Call Center, Credit Monitoring, etc.)

Public Relations

Data Recovery

Ransom Payments

Resulting Lawsuits

What’s Not Insured:

Downtime

Disruption

Community Relations

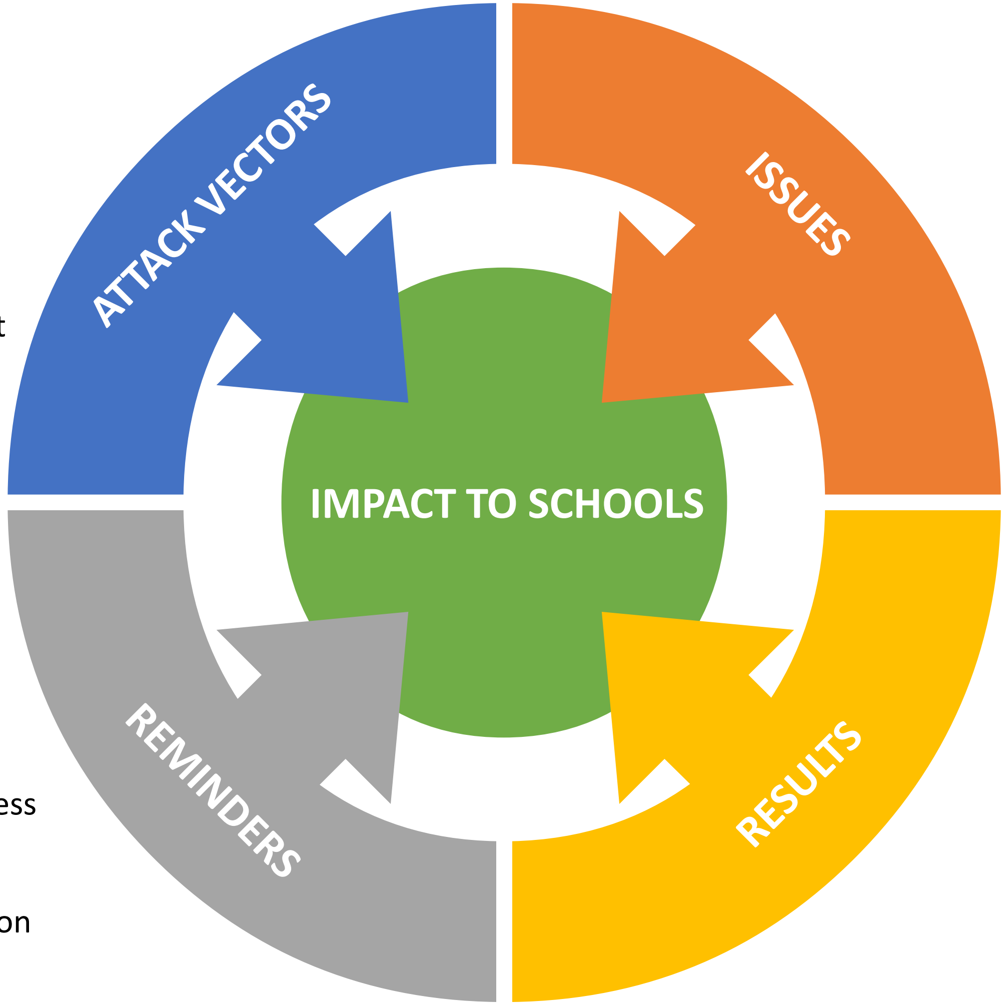
Staff Relations

Reputational Damage

Case Studies

Cyber Attack Cases

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



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

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

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

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

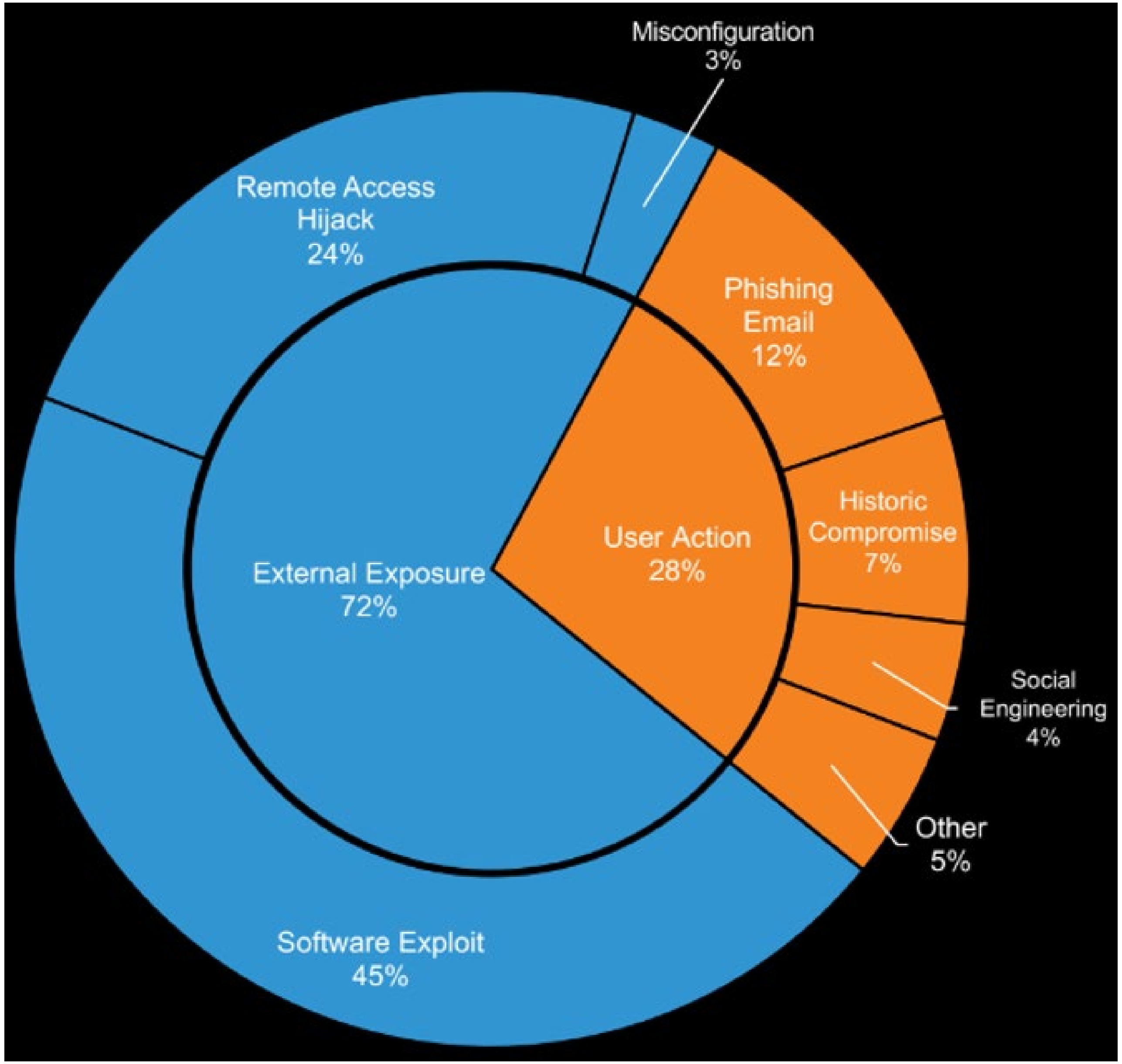
Root Point of Compromise

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 system and gained access to the network or data
    - Easiest method; widely used

- User Action
  - Attacker gained access due to a user’s action (opening malicious file, re-using passwords, social engineering)



Source: Arctic Wolf Networks

External Exposure

Software exploit

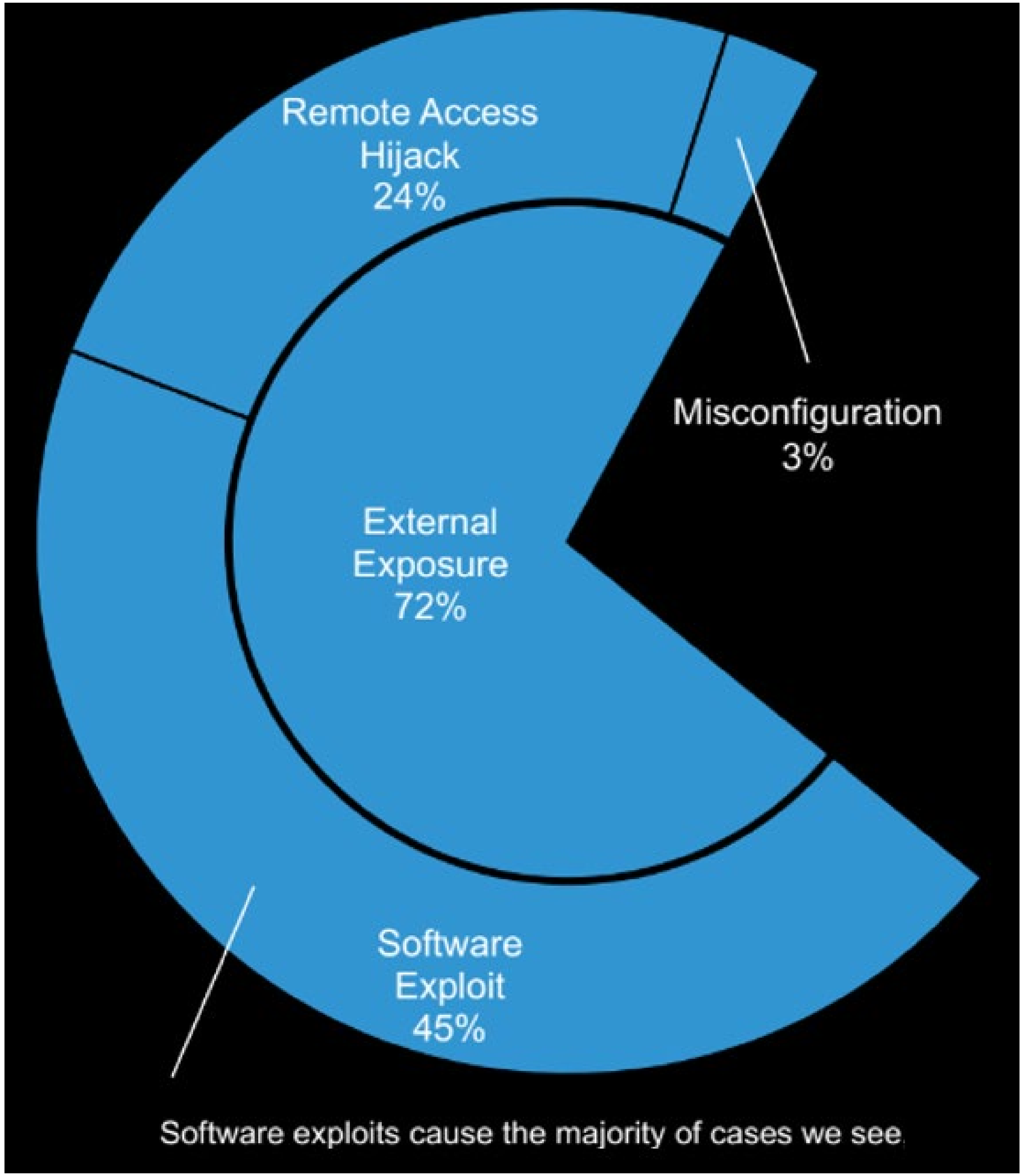
- 45% of incidents caused by vulnerabilities that could have been mitigated through security updates

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



Software exploits cause the majority of cases we see.

Source: Arctic Wolf Networks

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

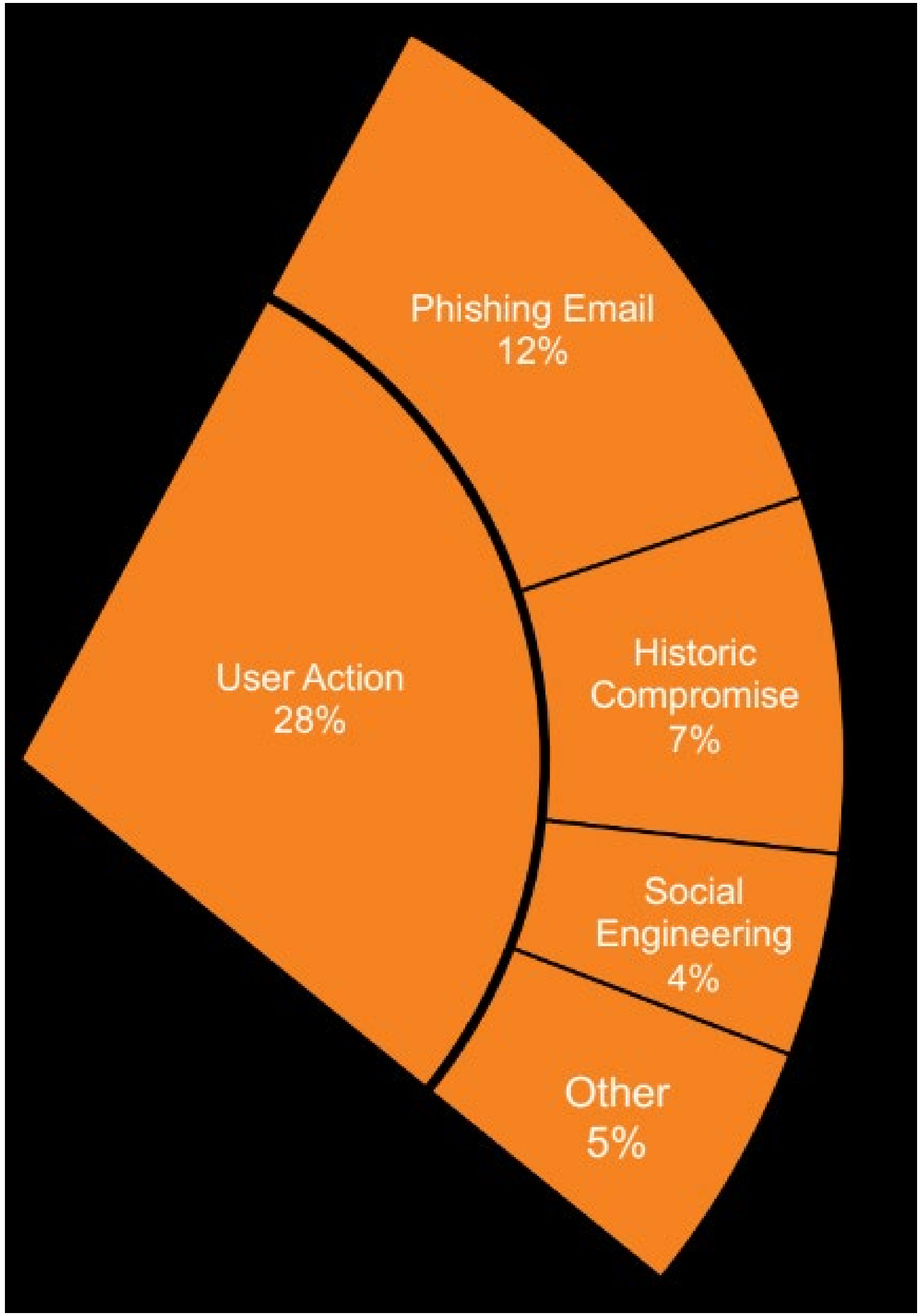
Social engineering

- 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.



Source: Arctic Wolf Networks

The Process of a Ransomware Claim

Ransomware

The Process

Pre-Incident

Develop response plan

Performing backups

Conducting training

External vulnerability reports

Evaluate and assess damage

Viable backups

Do NOT pay ransom

Recover from backups

Evaluate and assess damage

Backups not viable

Decide to pay ransom or not

Payment should provide encryption key

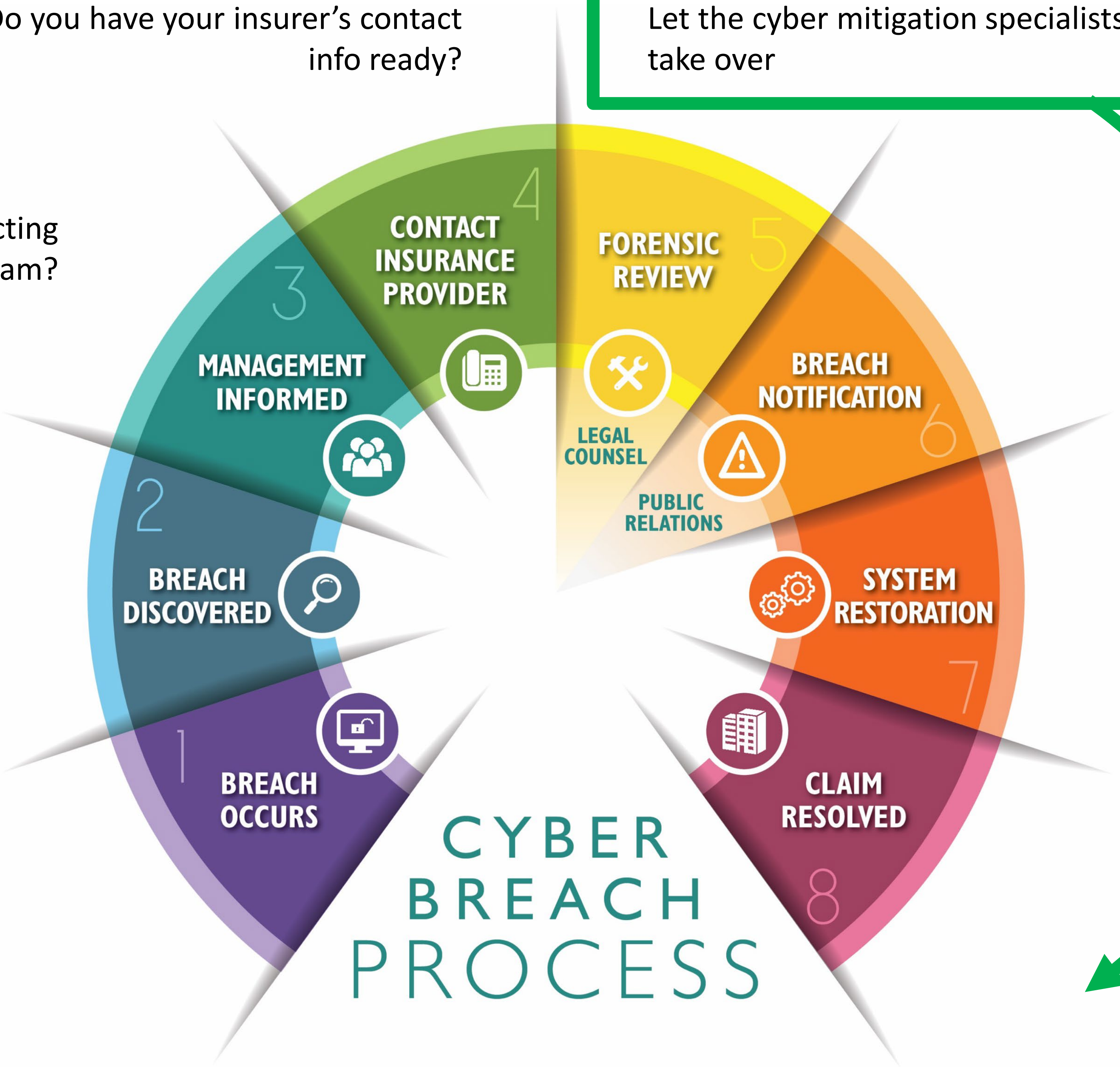
Recover

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



Resources

ESSENTIAL
CYBERSECURITY
PRACTICES FOR K12

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

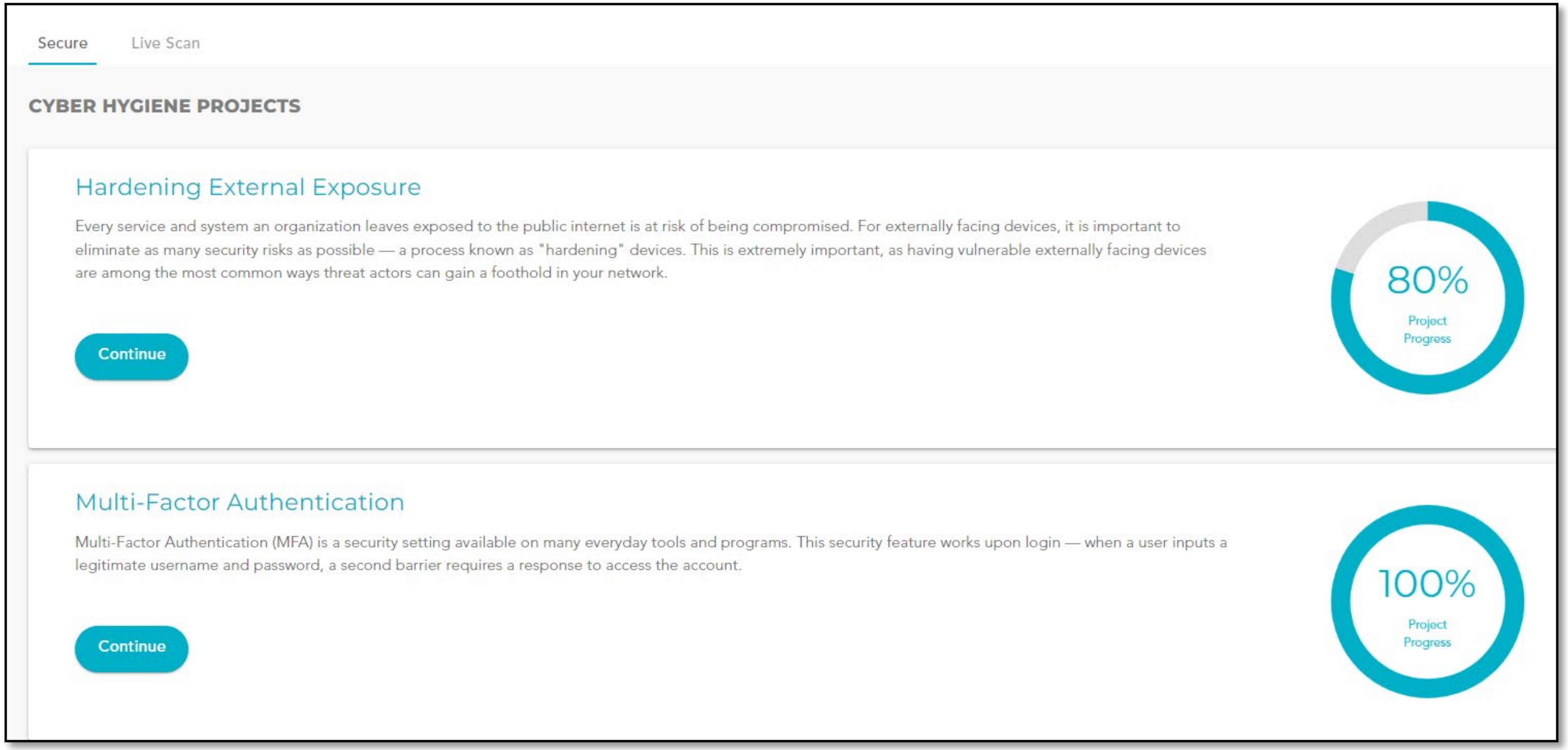
KnowBe4
Human error. Conquered.

MISecure.org

VECTOR SOLUTIONS | SafeSchools

EduPaths Training

Tetra Defense – MyCyber Platform



CYBER HYGIENE PROJECTS

Hardening External Exposure

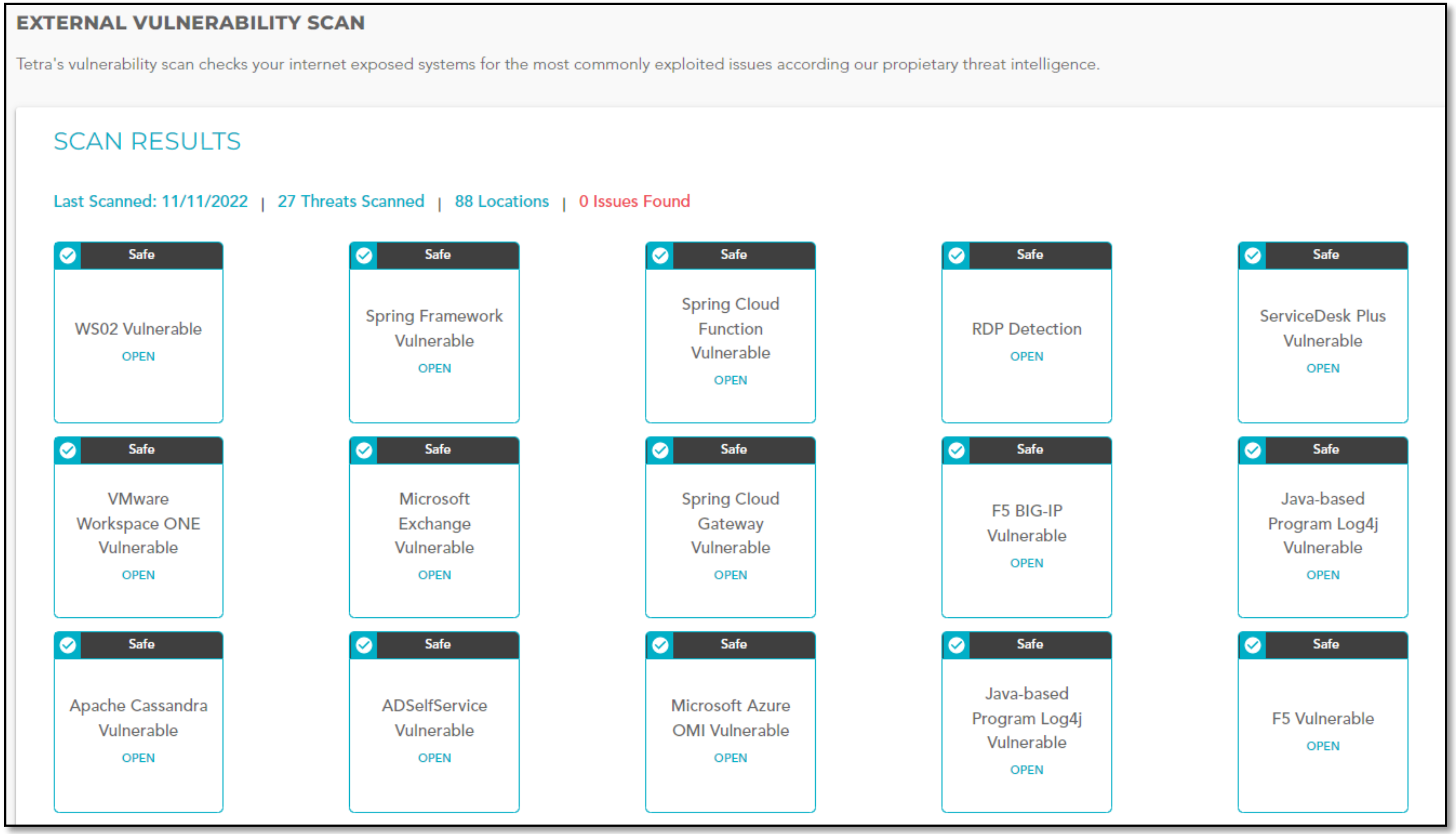
Every service and system an organization leaves exposed to the public internet is at risk of being compromised. For externally facing devices, it is important to eliminate as many security risks as possible — a process known as "hardening" devices. This is extremely important, as having vulnerable externally facing devices are among the most common ways threat actors can gain a foothold in your network.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security setting available on many everyday tools and programs. This security feature works upon login — when a user inputs a legitimate username and password, a second barrier requires a response to access the account.

Top 10 Cyber Hygiene Projects

Tetra Defense – MyCyber Platform



EXTERNAL VULNERABILITY SCAN

Tetra's vulnerability scan checks your internet exposed systems for the most commonly exploited issues according our propietary threat intelligence.

SCAN RESULTS

Last Scanned: 11/11/2022 | 27 Threats Scanned | 88 Locations | 0 Issues Found

✓ Safe
WS02 Vulnerable
OPEN

✓ Safe
Spring Framework Vulnerable
OPEN

✓ Safe
Spring Cloud Function Vulnerable
OPEN

✓ Safe
RDP Detection
OPEN

✓ Safe
ServiceDesk Plus Vulnerable
OPEN

✓ Safe
VMware Workspace ONE Vulnerable
OPEN

✓ Safe
Microsoft Exchange Vulnerable
OPEN

✓ Safe
Spring Cloud Gateway Vulnerable
OPEN

✓ Safe
F5 BIG-IP Vulnerable
OPEN

✓ Safe
Java-based Program Log4j Vulnerable
OPEN

✓ Safe
Apache Cassandra Vulnerable
OPEN

✓ Safe
ADSelfService Vulnerable
OPEN

✓ Safe
Microsoft Azure OMI Vulnerable
OPEN

✓ Safe
Java-based Program Log4j Vulnerable
OPEN

✓ Safe
F5 Vulnerable
OPEN

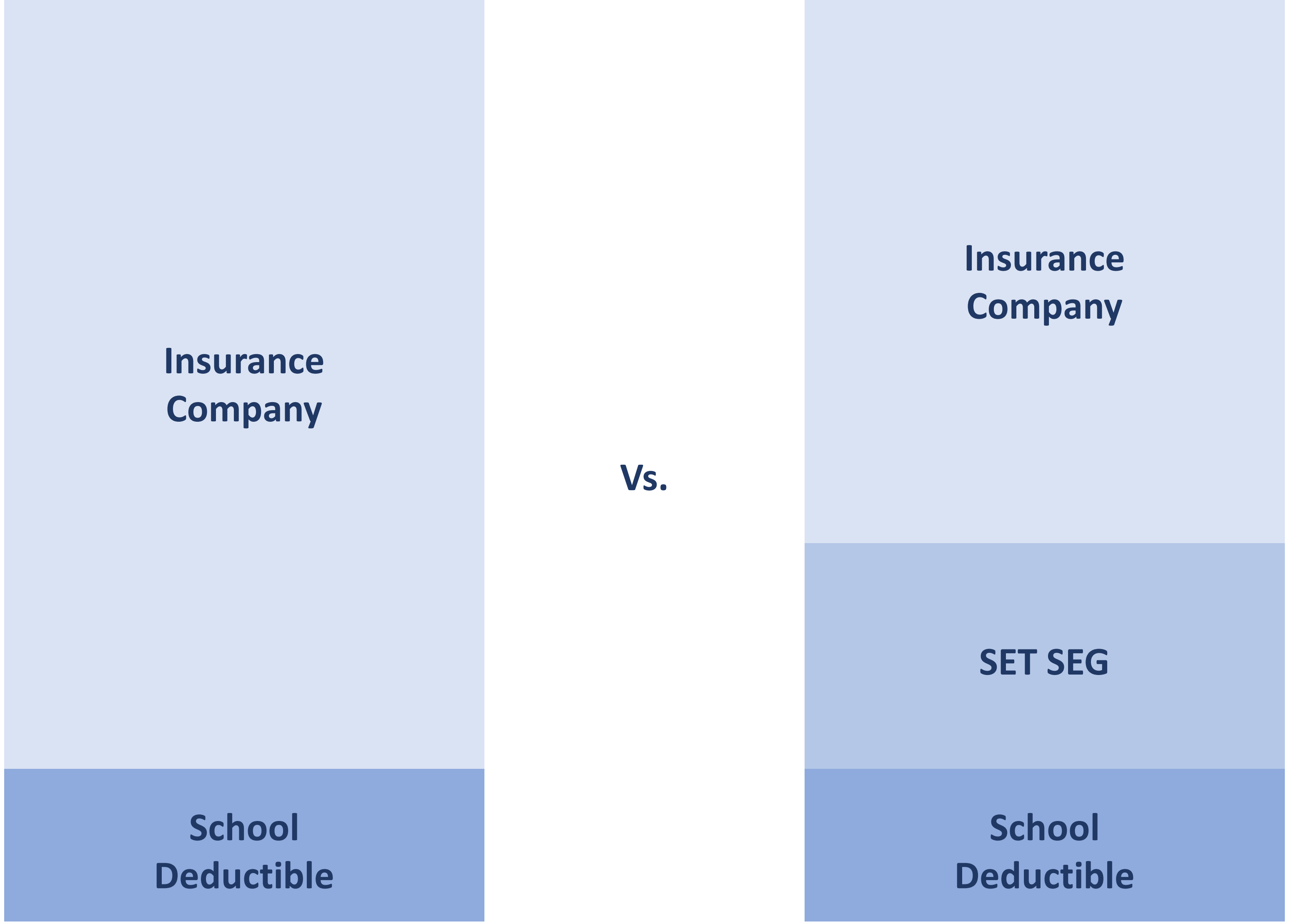
Monthly External Vulnerability Scan

Tetra Defense – MyCyber Platform

External Vulnerability Scans are….

Cyber Security Landscape

Insurance Structure



Insurance Company

School Deductible

Traditional Insurance

Vs.

Insurance Company

SET SEG

School Deductible

SET SEG Member

Typical Requirements

Multi-Factor Authentication

- Email
- Privileged user accounts

Backups

- In place / tested / stored separately / encrypted / anti-virus
- Tested 2x a year
- Ability to bring up within 24–72 hours

Email

- Monthly phishing tests
- Advanced threat protection for O365

Patching

- Critical & high-severity patches installed within 1–7 days

Typical Requirements

Remote Desktop Protocol (RDP)

- MFA enabled VPN access
- Network level authentication enabled

Planning & Policies

- Incident response plan (IR)
- Disaster recovery plan (DR)
- Business continuity plan (BC)

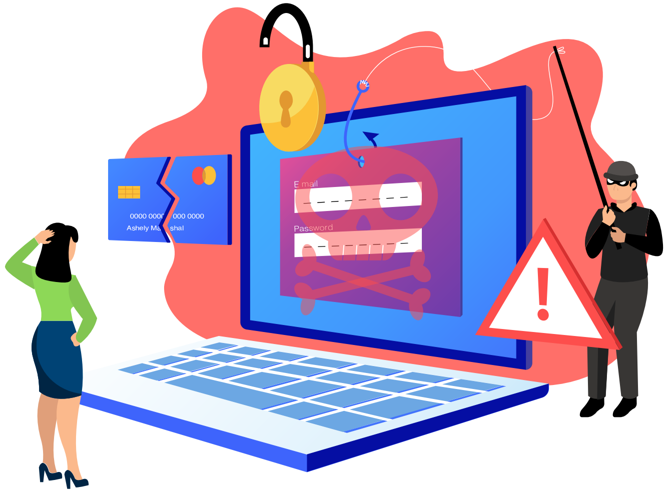
Endpoint Protection & Response

- Minimum: End-point protection (EPP) solution
- Preferred: End-point detection & response (EDR)

User Authority

- No “administrative rights” for staff

Cyber Insurance Changes?



Limited Market

Less appetite in the marketplace – will drive increased costs

Increase Deductibles

Substantial increase in the marketplace

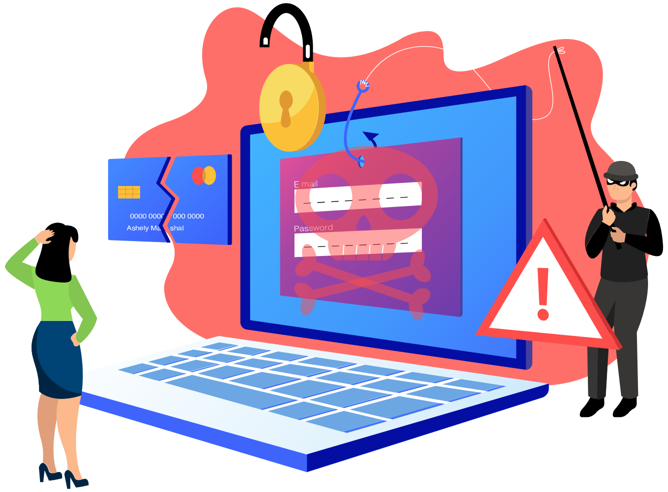
Coinsurance

District paying for portion of claim cost

Vulnerability Testing

Testing to conduct risk analysis

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

Future Requirements From the Insurance Industry

BUSINESS INSURANCE

www.businessinsurance.com

MAY 2021

SPECIAL REPORT

CLAIMS MANAGEMENT

PAGE 22

RANSOMWARE PROTECTIONS

Cyber defenses need rethink as hackers step up attacks

Phishing training

Multifactor authentication (MFA) – remote access / critical information

Backups offline / inaccessible to outsiders / encrypted / regularly scheduled

Endpoint protection and response (EDR)

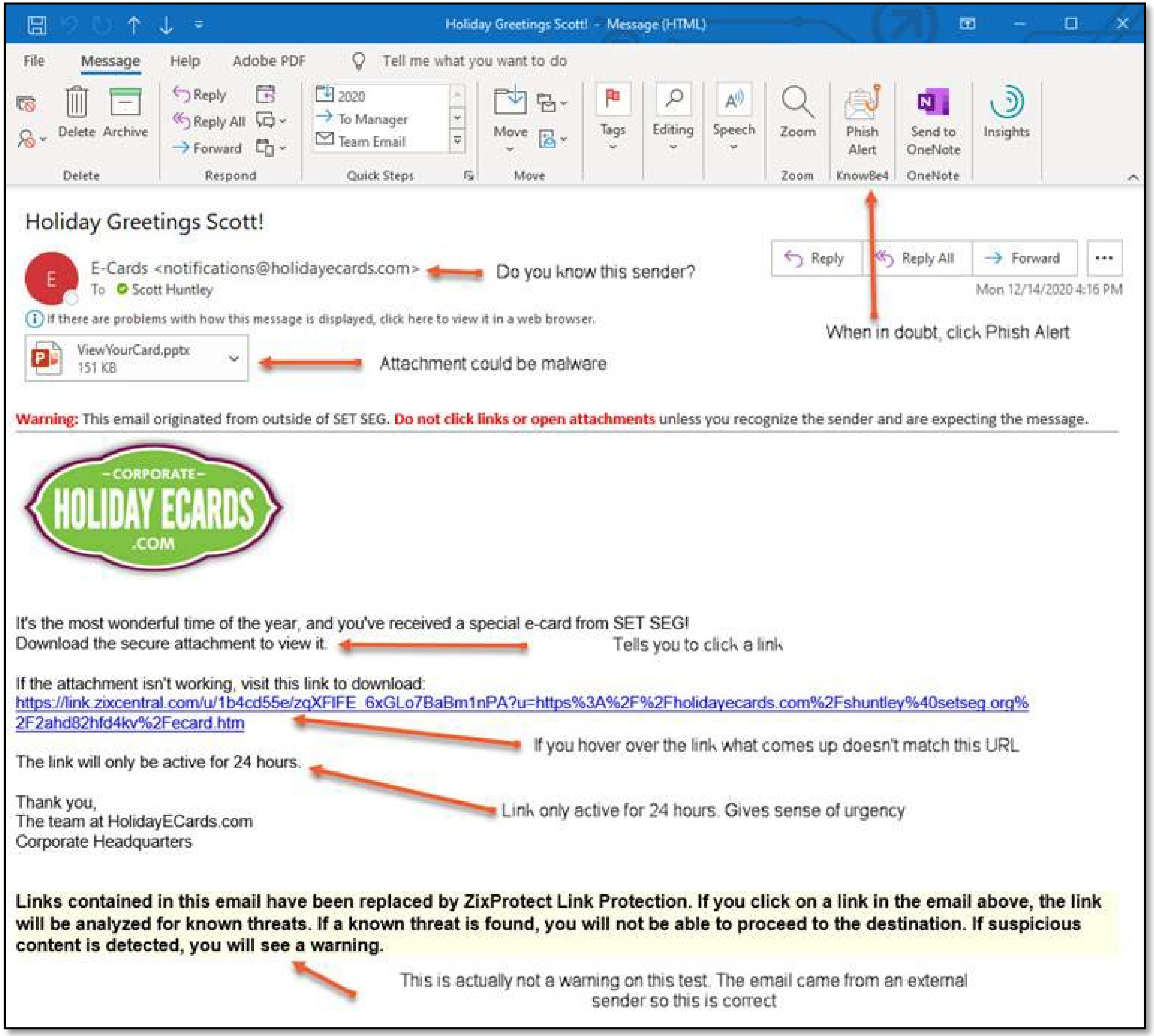
Limiting administrative access

System security patches updated

Close open ports

Vulnerability scans are coming…

Phishing



Holiday Greetings Scott!

E-Cards <notifications@holidayecards.com>

To Scott Huntley

Mon 12/14/2020 4:16 PM

Do you know this sender?

When in doubt, click Phish Alert

If there are problems with how this message is displayed, click here to view it in a web browser.

Attachment could be malware

Warning: This email originated from outside of SET SEG. **Do not click links or open attachments** unless you recognize the sender and are expecting the message.

It's the most wonderful time of the year, and you've received a special e-card from SET SEG!
Download the secure attachment to view it.

Tells you to click a link

If the attachment isn't working, visit this link to download:
https://link.zixcentral.com/u/1b4cd55e/zqXFIFE_6xGLo7BaBm1nPA?u=https%3A%2F%2Fholidayecards.com%2Fshuntley%40setseg.org%2F2ahd82hfd4kv%2Fecard.htm

If you hover over the link what comes up doesn't match this URL

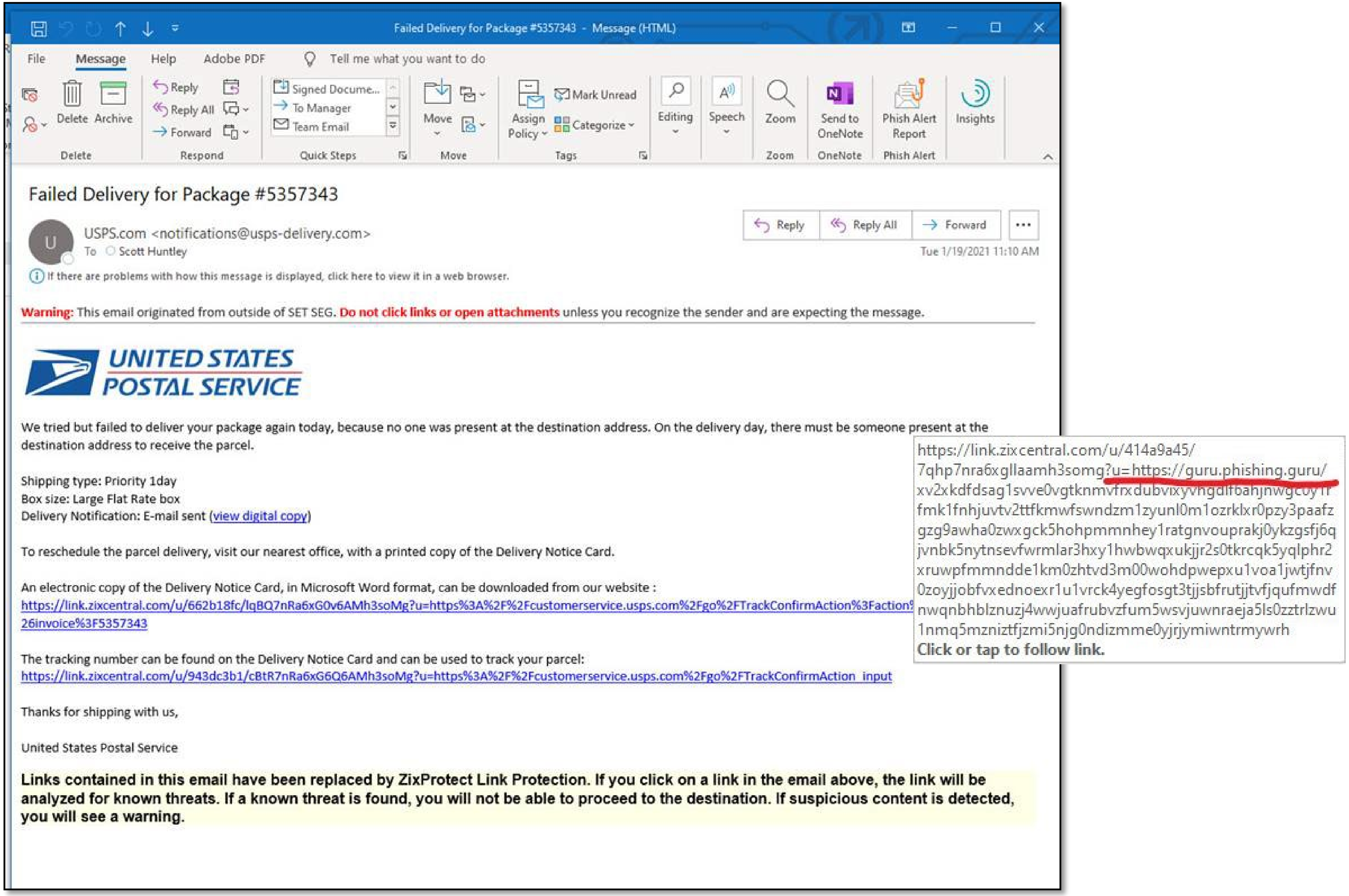
The link will only be active for 24 hours.

Link only active for 24 hours. Gives sense of urgency

Thank you,
The team at HolidayECards.com
Corporate Headquarters

Links contained in this email have been replaced by ZixProtect Link Protection. If you click on a link in the email above, the link will be analyzed for known threats. If a known threat is found, you will not be able to proceed to the destination. If suspicious content is detected, you will see a warning.

This is actually not a warning on this test. The email came from an external sender so this is correct



Failed Delivery for Package #5357343

USPS.com <notifications@usps-delivery.com>
To Scott Huntley
Tue 1/19/2021 11:10 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Warning: This email originated from outside of SET SEG. **Do not click links or open attachments** unless you recognize the sender and are expecting the message.

UNITED STATES POSTAL SERVICE

We tried but failed to deliver your package again today, because no one was present at the destination address. On the delivery day, there must be someone present at the destination address to receive the parcel.

Shipping type: Priority 1day
Box size: Large Flat Rate box
Delivery Notification: E-mail sent (view digital copy)

To reschedule the parcel delivery, visit our nearest office, with a printed copy of the Delivery Notice Card.

An electronic copy of the Delivery Notice Card, in Microsoft Word format, can be downloaded from our website :
https://link.zixcentral.com/u/662b18fc/lqBQ7nRa6xG0v6AMh3soMg?u=https%3A%2F%2Fcustomerservice.usps.com%2Fgo%2FTrackConfirmAction%3Faction%26invoice%3F5357343

The tracking number can be found on the Delivery Notice Card and can be used to track your parcel:
https://link.zixcentral.com/u/943dc3b1/cBtR7nRa6xG6Q6AMh3soMg?u=https%3A%2F%2Fcustomerservice.usps.com%2Fgo%2FTrackConfirmAction_input

Thanks for shipping with us,

United States Postal Service

Links contained in this email have been replaced by ZixProtect Link Protection. If you click on a link in the email above, the link will be analyzed for known threats. If a known threat is found, you will not be able to proceed to the destination. If suspicious content is detected, you will see a warning.

https://link.zixcentral.com/u/414a9a45/
7qhp7nra6xgllaamh3somg?u=https://guru.phishing.guru/
xv2xkdfdsag1svve0vgtknmvfrxdubvixyvhgdlfbahjnwgcoy1f
fmk1fnhjuvtv2ttfkmwfswndzm1zyunl0m1ozrklxr0pzy3paafz
gzg9awha0zwxgck5hohpmmnhey1ratgnvouprakj0ykzgsfj6q
jvnbk5nytnsevfwrmlar3hxy1hwbwqxukjjr2s0tkrcqk5yqlphr2
xruwpfmmndde1km0zhtvd3m00wohdpwepxu1voa1jwtjfnv
0zoyjjobfvxednoexr1u1vrck4yegfosgt3tjjsbfrutjjtvfjqufmwdf
nwqnbhblznuzj4wwjuafrubvzfum5wsvjuwnraeja5ls0zztrlzwu
1nmq5mzniztfjzmi5njg0ndizmme0yjrjymiwntrmywrh
Click or tap to follow link.

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

Contact

Emergency Contact

☎ 800-292-5421
After Hours, Press 1

Paul Grienke

Insurance Education Specialist

☎ 517-881-4603

✉ pgrienke@setseg.org

Steve Privasky

Associate Administrator – PC and WC

☎ 231-670-3700

✉ sprivasky@setseg.org