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

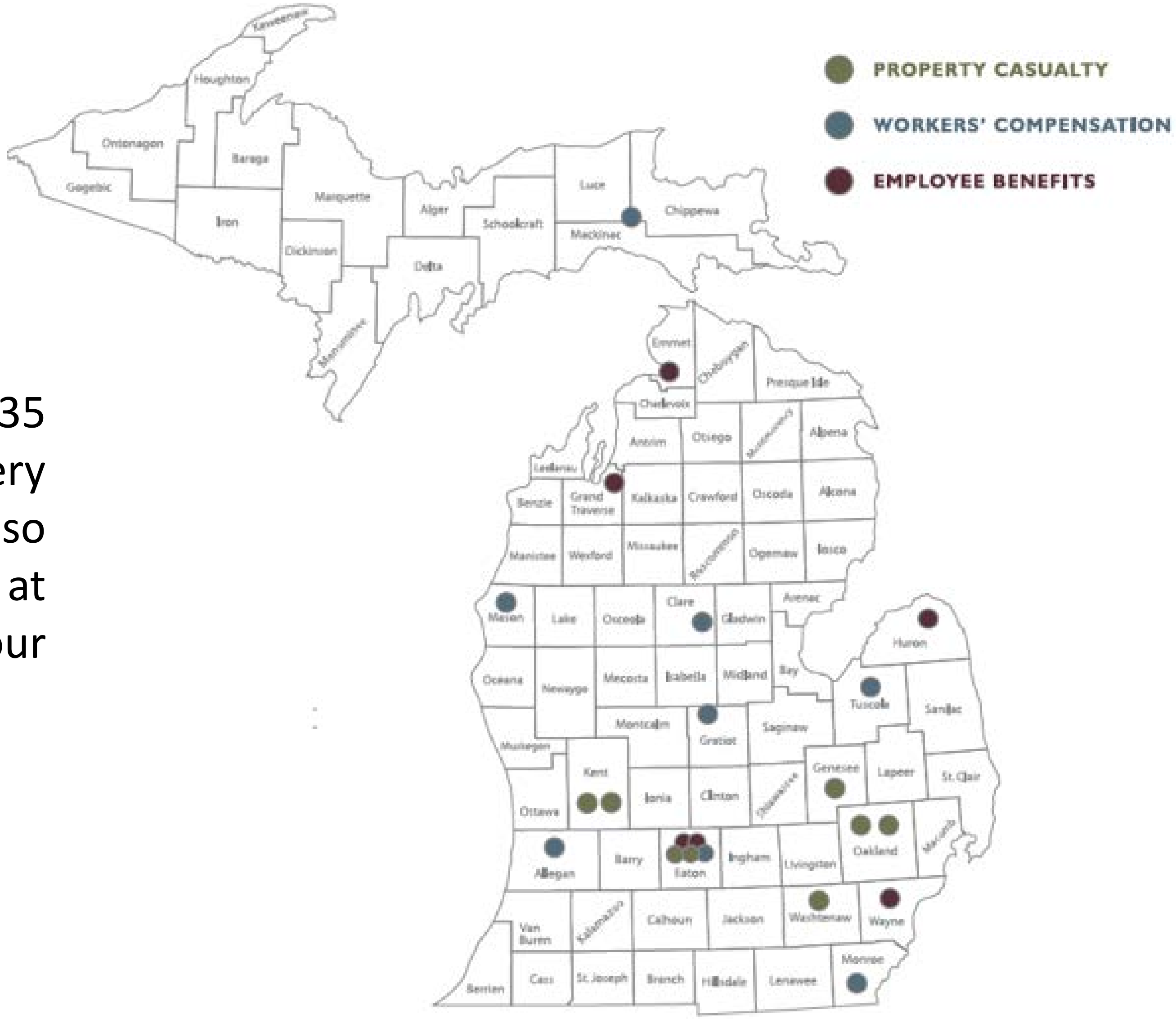
- Healthcare, Dental, Vision and Long-Term Disability
- Consulting, compliance and administration services

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

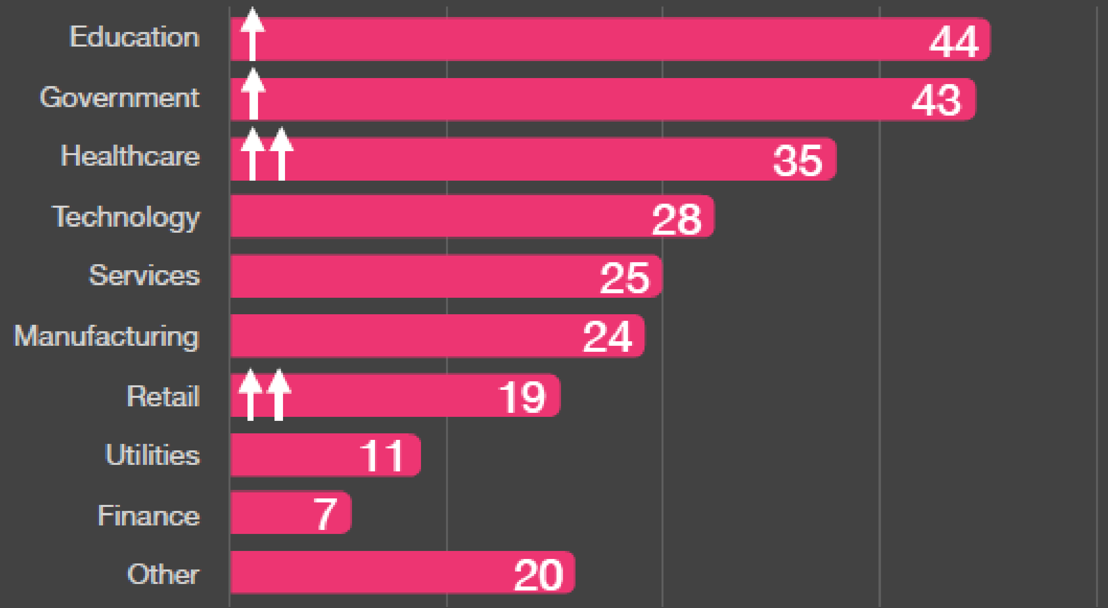
Community Relations

Staff Relations

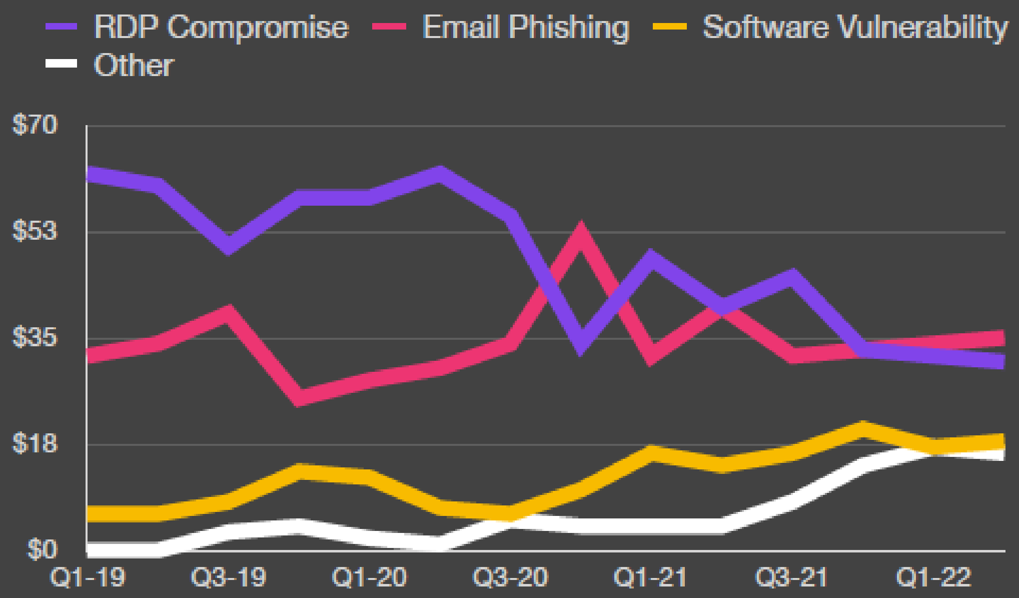
Reputational Damage

September 2022 – Industry Stats

Ransomware by Industry



Attack Vectors[2]



[2] Courtesy Coveware

CASE STUDIES

Case Study #1 | K-12 District – Enrollment 1,200+

Days to Report:

18 days

Attack Vector:

Employee, via remote connection, clicked on malicious link

Issue: District attempted to manage breach internally

Result: Threat actor hit district with a second attack, $300,000 ransom demand

Reminders: Use VPN, use MFA, report claims immediately

Case Study #2 | K-12 District – Enrollment 5,000+

Days to Report:	Attack Vector:
30 days	Email (social engineering)

Issue: Threat actor pretended to be the superintendent

Result: Wire transferred $154,000 and $169,000 to fraudulent vendor

Reminders: Checks and balances

Case Study #3 | K-12 District – Enrollment 2,000+

Days to Report:

0 days

Attack Vector:

Email (ransomware attack)

Issue: District’s 14 servers and 400 workstations were nonoperational. No offline backups to recover from.

Result: Negotiation with threat actor demanding $196,000. District’s deductible now $250,000 until MFA and vulnerability scans are implemented.

Reminders: backup strategy, MFA, phishing training, and be aware of what data you are hosting.

Case Study #4 | K-12 District – Enrollment 10,000+

Days to Report:	Attack Vector:
0 days	Threat actor monitoring RDP connection, deployed a malicious Microsoft Word/Excel document through email phishing resulting in ransomware

Issue: District’s 80 servers were impacted. Backups were not infected.

Result: Did not pay ransom demand of $640,000. Slow moving process to work through legal, forensics, notification logistics.

Reminders: backup strategy, phishing training, and be aware of any communication with the threat actor and what the local news reports.

Case Study #5 | ISD – Annual Revenue $20M

Days to Report:

14 days

Attack Vector:

Email phishing to facilities employee, posing as charity

Issue: Employee entered credentials; hacker changed rules in inbox. Phishing emails then sent from that inbox to neighboring districts.

Result: No data exfiltrated, no data compromised. Time, energy, reputational damage, and approximately $25,000 in insurance claims.

Reminders: Phishing training (all staff), protect systems with MFA for ALL staff.

Case Study #6 | K-12 District – Enrollment 5,000+

Days to Report:

0 days

Attack Vector:

Gained student credentials, accessed student server and with no segmentation of networks, jumped into administration account

Issue: Backups were encrypted

Result: School paid over $500,00 ransom as this was a double-layer encryption. School now has $250,000 deductible until MFA is implemented for ALL staff (at time only Administrators had MFA).

Reminders: Network segmentation, EDR for detection and response

Case Study #7 | K-12 District – Enrollment 3,000+

Days to Report:

0 days (December 26th)

Attack Vector:

Attacker gained access via RDP, installed ransomware

Issue: Disruptive and potential loss of student data.

Result: Total claim was only $58,000 (no ransom paid). However, this was district’s second cyber claim – current deductible is now $250,000 until MFA and EDR are implemented.

Reminders: MFA and EDR tools

Case Study #8 | Annual Revenue – $170M

Days to Report:

5 days

Attack Vector:

Email (social engineering)

Issue: Attacker spoofing Clark Construction emails, sent ACH change request for late payment

Result: ISD transferred $240,000 to fraudulent account – Clark Construction contacted district about outstanding payment

Reminders: Policies & procedures, call to verify

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

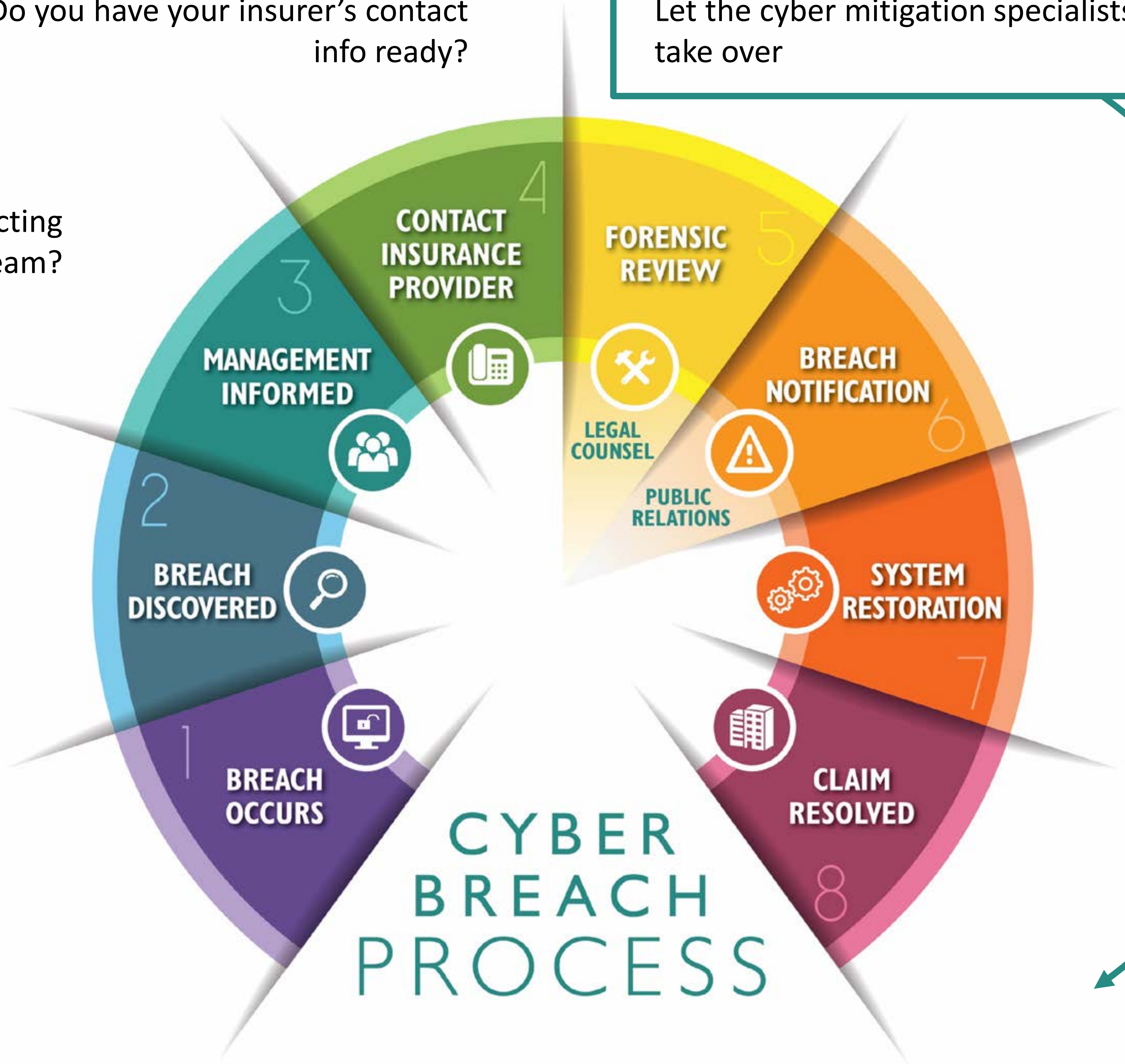
Recover

Do you have your insurer's contact info ready?

Let the cyber mitigation specialists take over

Who are you contacting within your team?

Incident Response Plan



Contact

	Emergency Contact	☎ 800-292-5421 *after hours press 1
	Amy Guilford Chief Program Administrator of PC/WC	☎ 517-816-1699 ✉ aguilford@setseg.org
	Tanya Charlow Director of Claims	☎ 517-816-1623 ✉ tcharlow@setseg.org
	Steve Privasky Associate Administrator of PC/WC	☎ 231-670-3700 ✉ sprivasky@setseg.org

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.

FOR MORE INFORMATION | MISECURE.ORG

misen MAISA merit

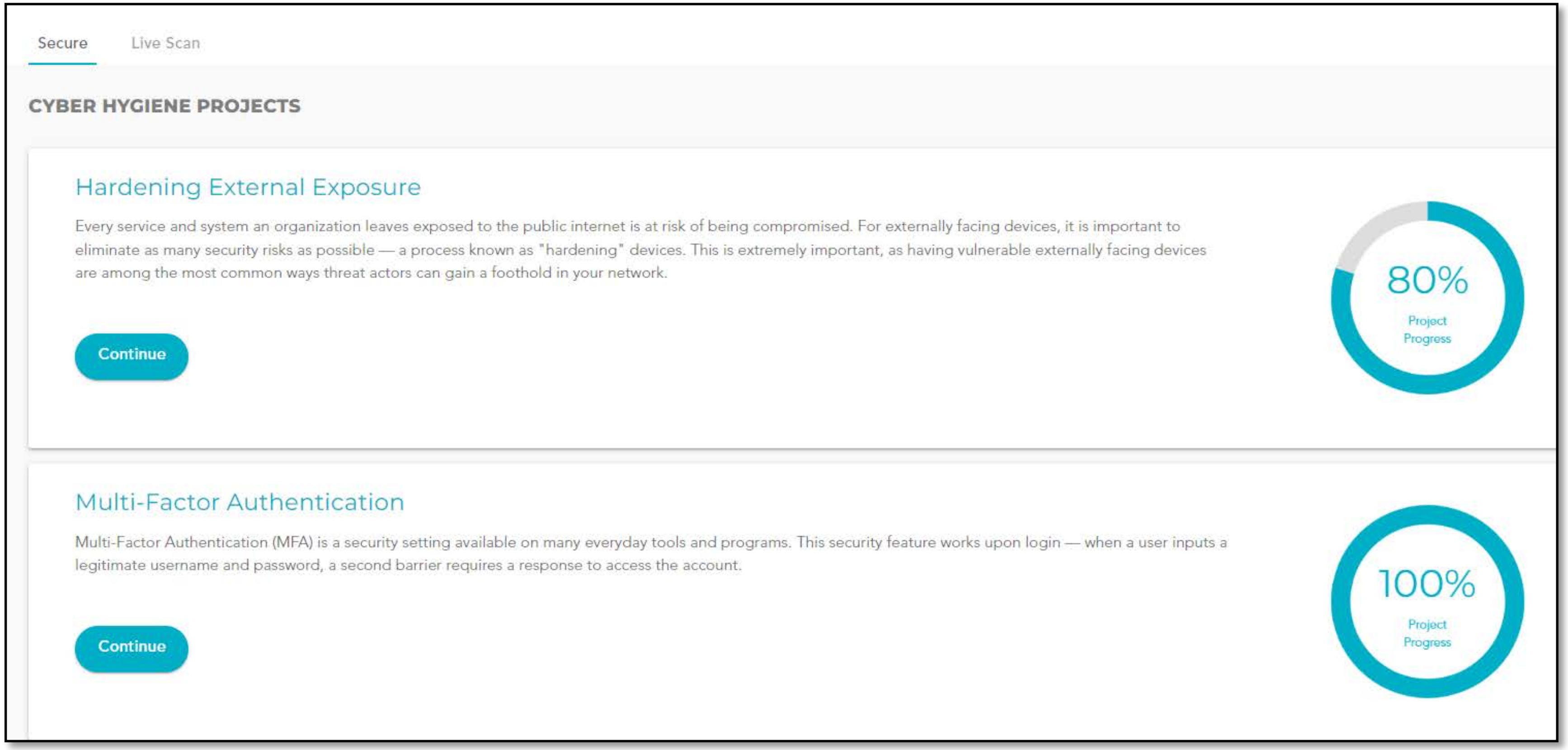
KnowBe4
Human error. Conquered.

MISecure.org

VECTOR SOLUTIONS | SafeSchools

EduPaths Training

Tetra Defense – MyCyber Platform



CYBER HYGIENE PROJECTS

Hardening External Exposure

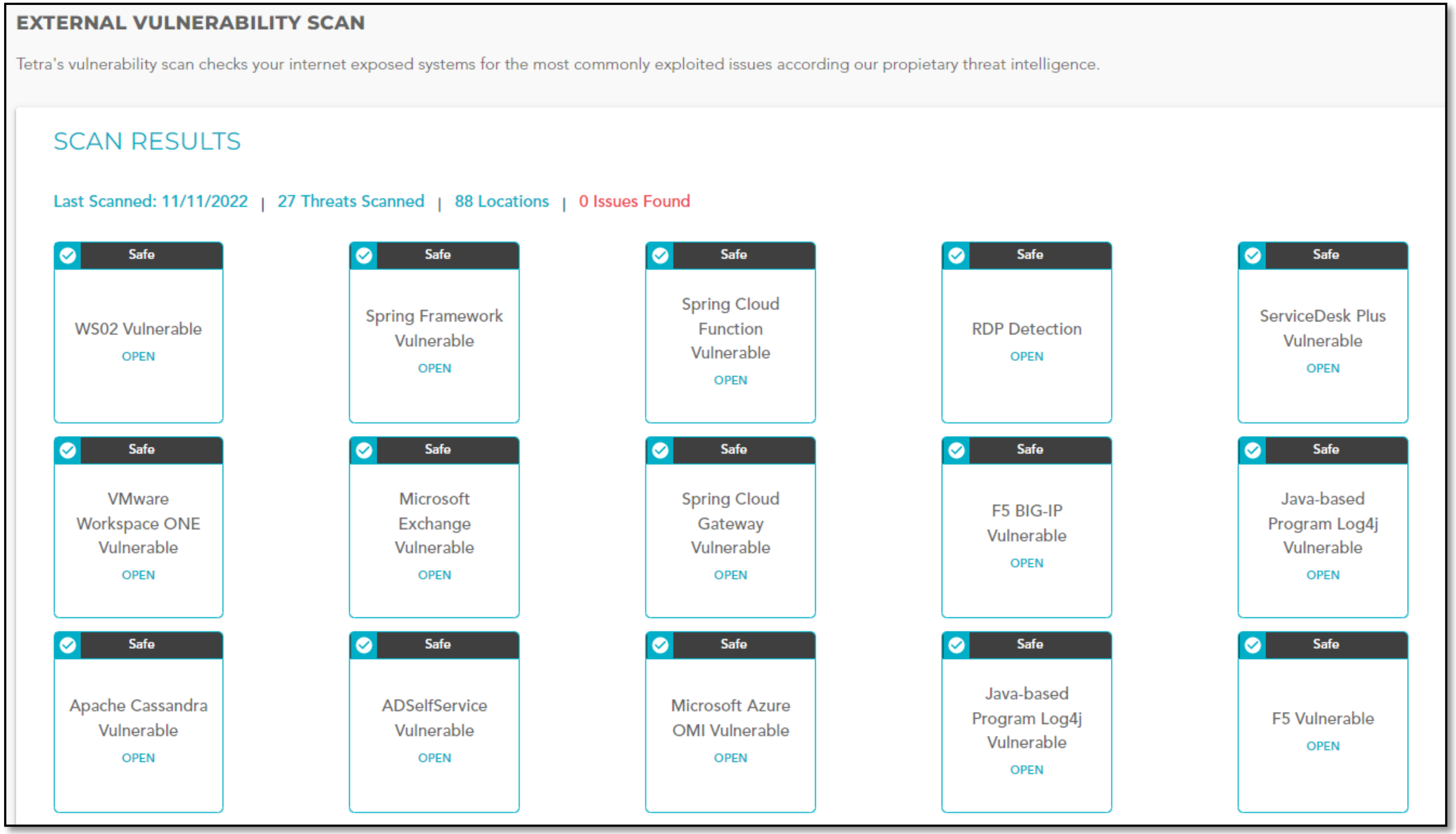
Every service and system an organization leaves exposed to the public internet is at risk of being compromised. For externally facing devices, it is important to eliminate as many security risks as possible — a process known as "hardening" devices. This is extremely important, as having vulnerable externally 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

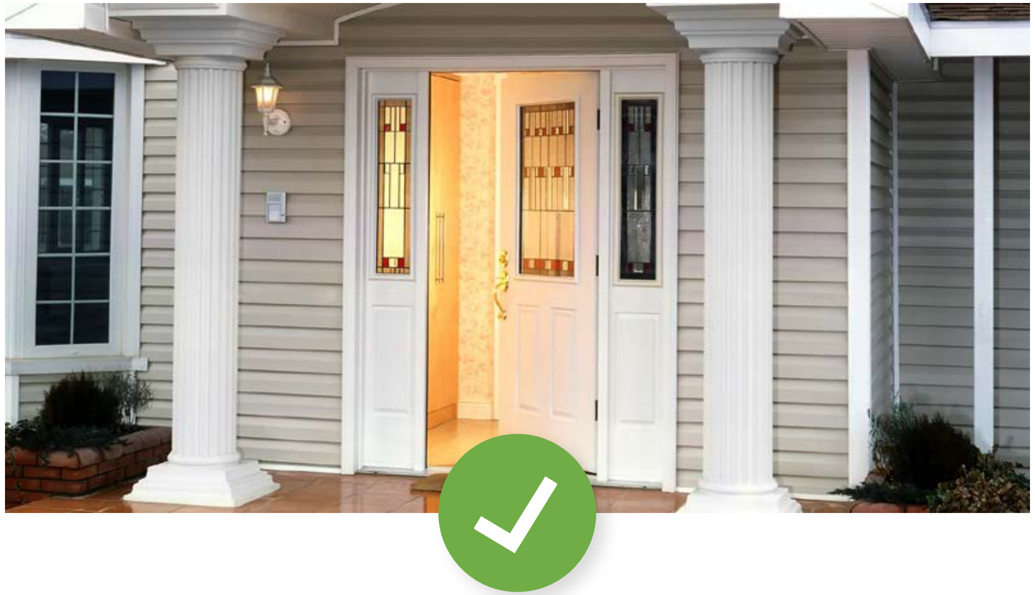
Last Scanned: 11/11/2022 | 27 Threats Scanned | 88 Locations | 0 Issues Found

✓ 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

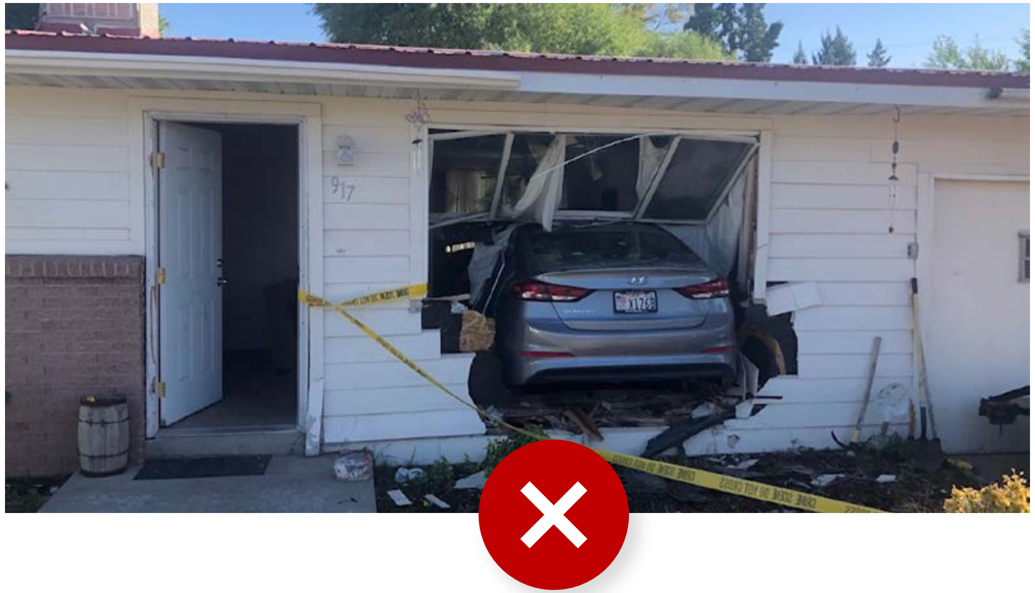
Monthly External Vulnerability Scan

Tetra Defense – MyCyber Platform

External Vulnerability Scans are….



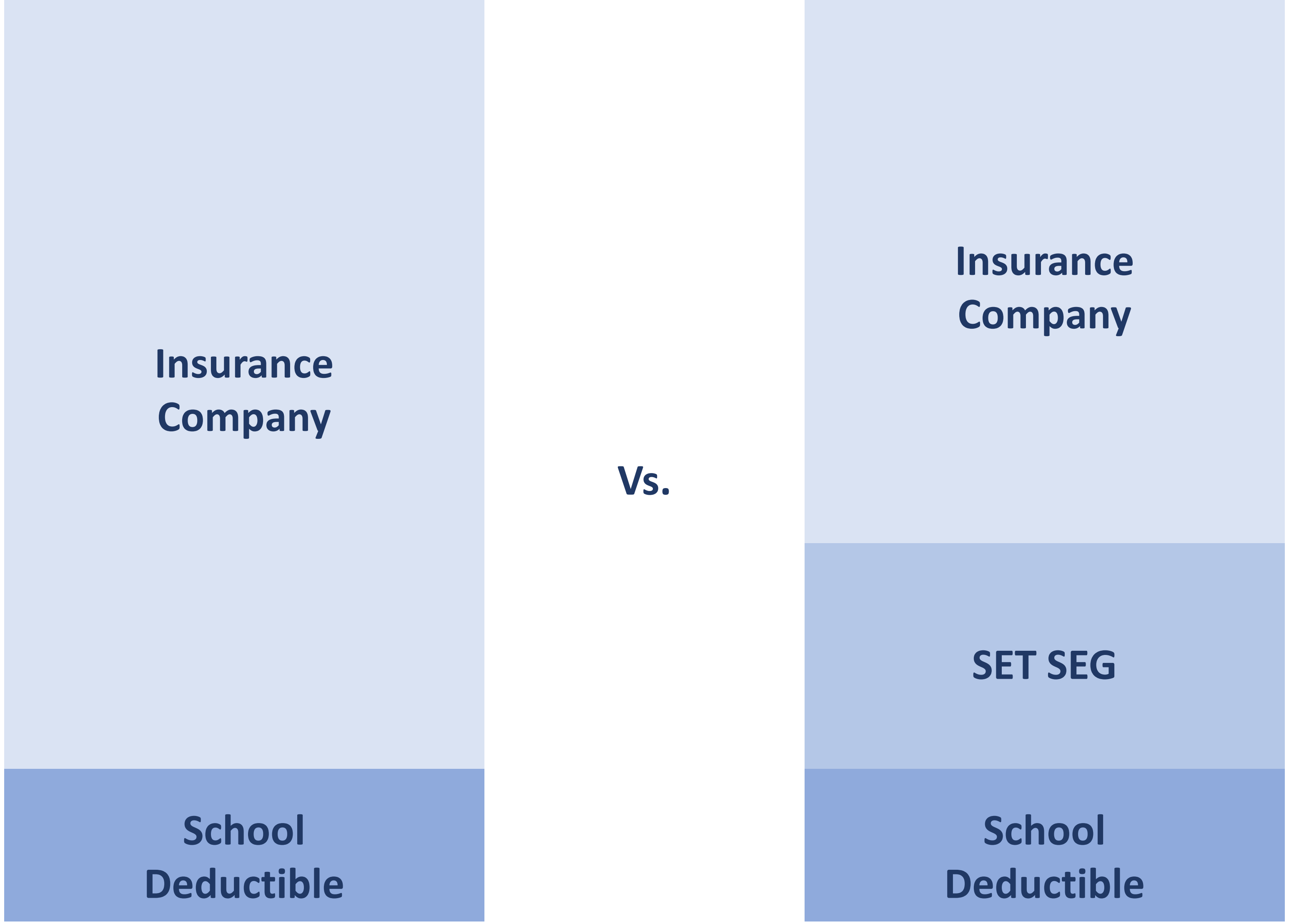
✓



✗

CYBER SECURITY LANDSCAPE

Insurance Structure



Traditional Insurance

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)

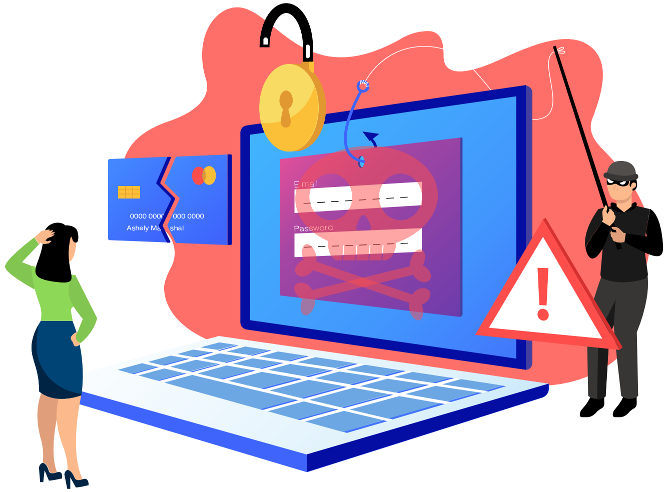
Endpoint Protection & Response

- 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

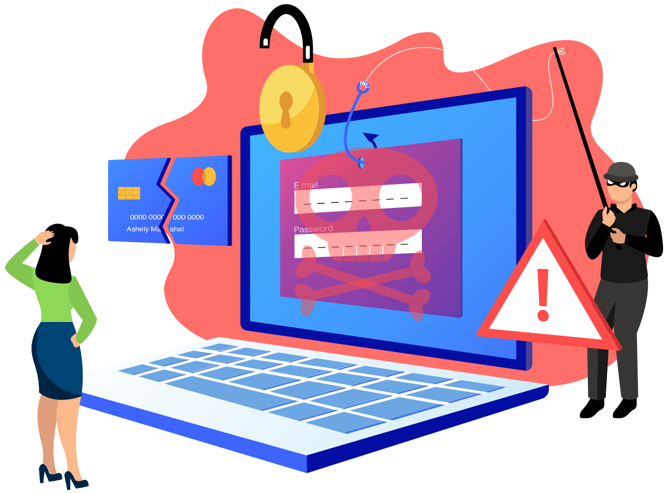
Coinsurance

District paying for portion of claim cost

Vulnerability Testing

Testing to conduct risk analysis

Cyber Insurance Changes?



Renewals

Application process more challenging

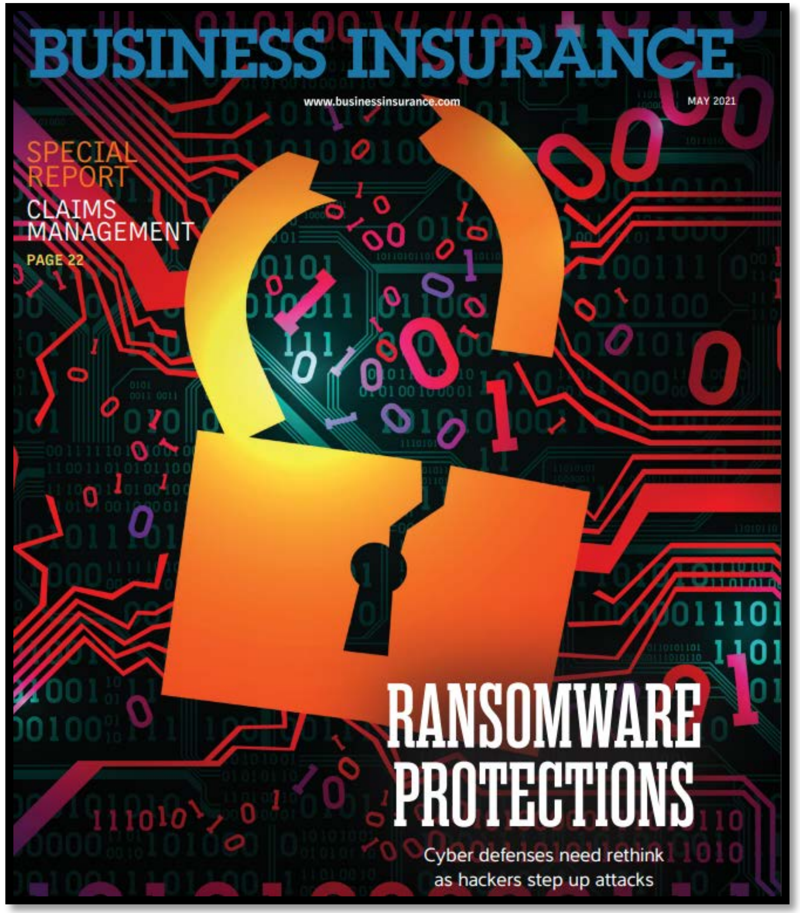
Lower Limits

Creating sublimit on amount of coverage

Extortion/Ransom

Coverage may cease to exist in the future

Future Requirements From the Insurance Industry



Phishing training

Multifactor authentication (MFA) – remote access / critical information

Backups offline / inaccessible to outsiders / encrypted / regularly scheduled

Endpoint protection and response (EDR)

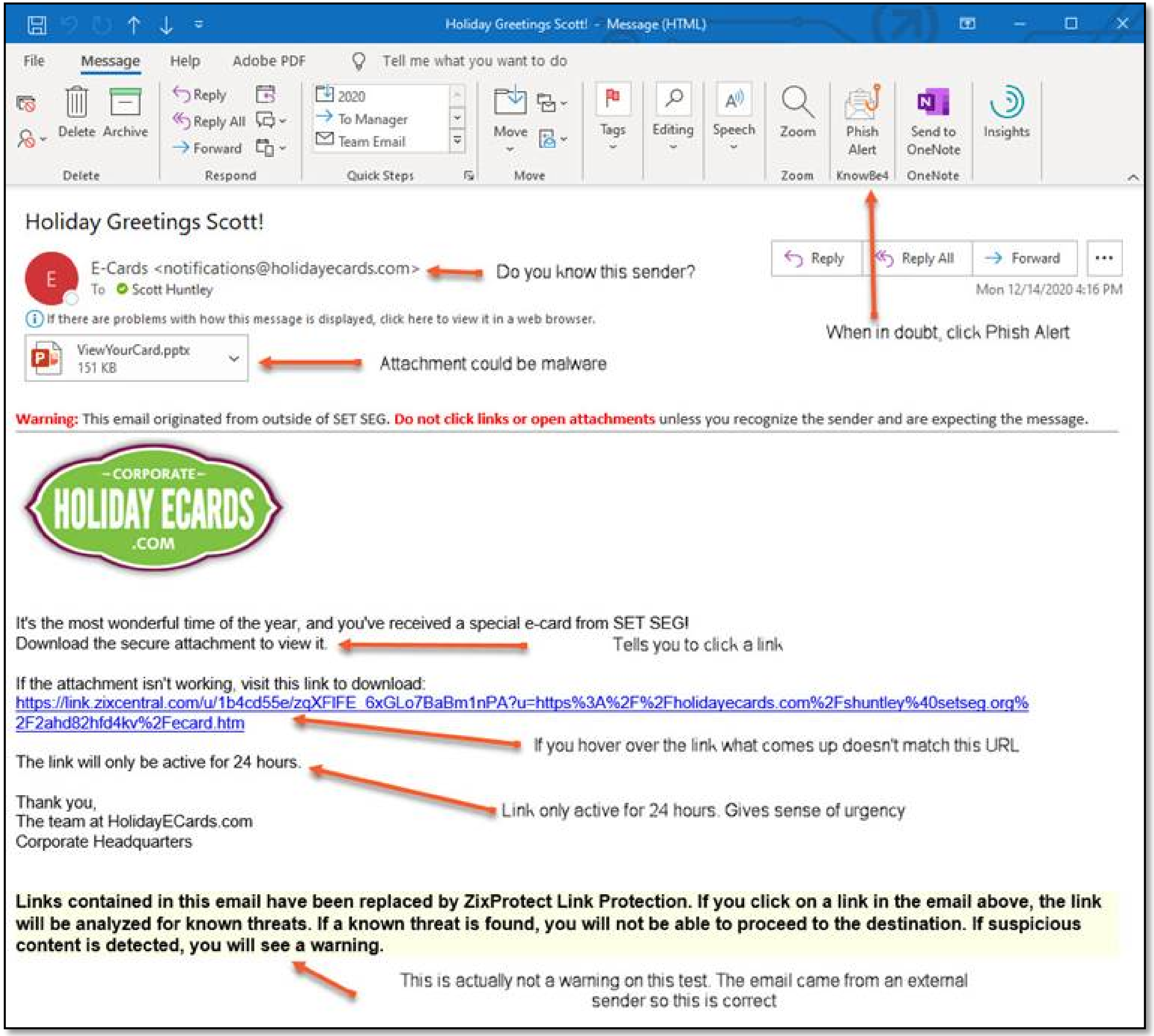
Limiting administrative access

System security patches updated

Close open ports

Vulnerability scans are coming…

PHISHING



Holiday Greetings Scott!

E-Cards <notifications@holidayecards.com>

Do you know this sender?

To Scott Huntley

Mon 12/14/2020 4:16 PM

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.

ViewYourCard.pptx
151 KB

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

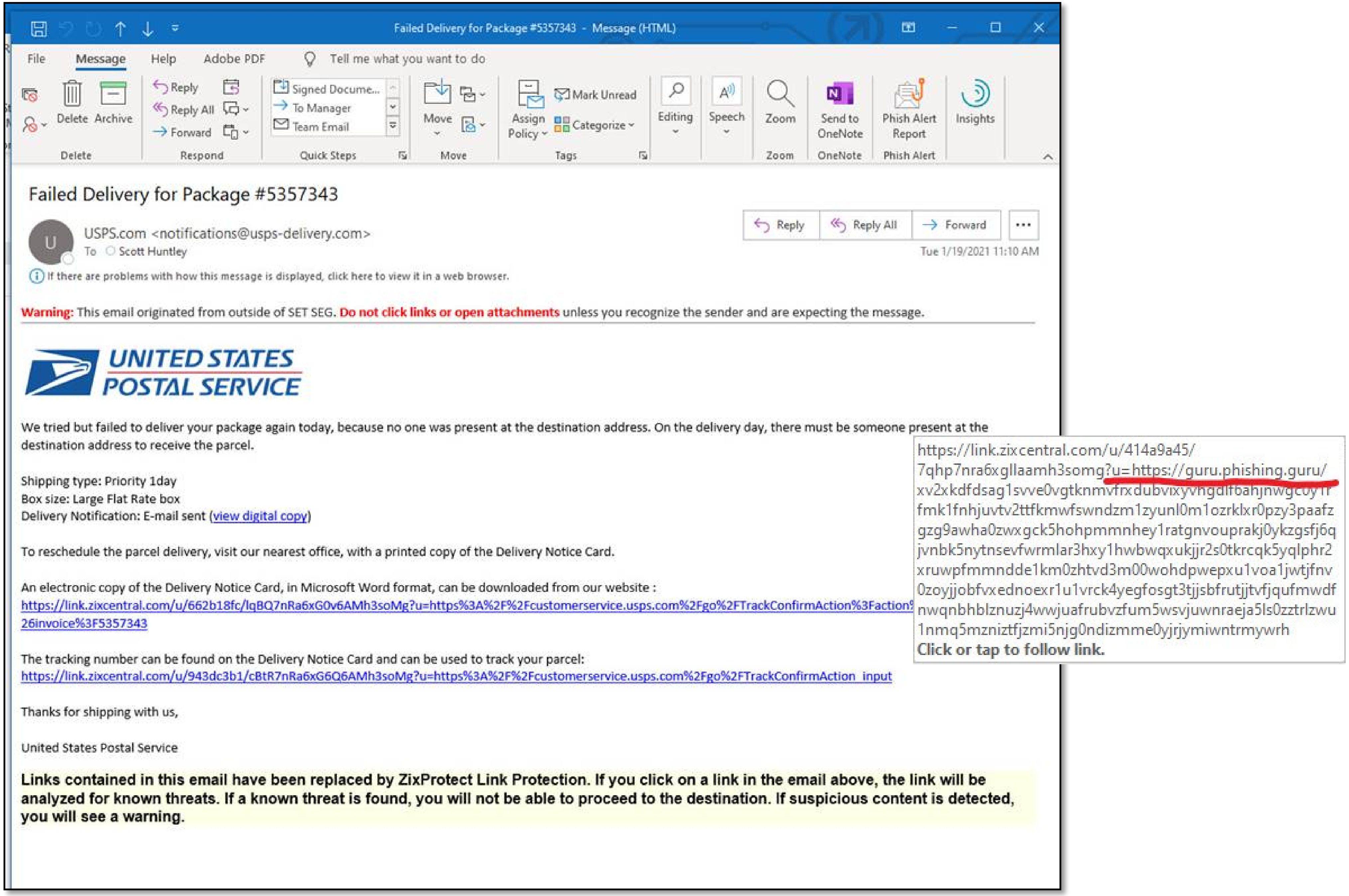
The link will only be active for 24 hours.

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/
xv2xkdfdsag1svve0vgtknmvfrxdubvixyvhgdlfbahjnwgc0y1f
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

Amy Guilford

Chief Program Administrator of PC/WC

☎ 517-816-1699

✉ aguilford@setseg.org

Tanya Charlow

Director of Claims

☎ 517-816-1623

✉ tcharlow@setseg.org

Steve Privasky

Associate Administrator of PC/WC

☎ 231-670-3700

✉ sprivasky@setseg.org