Benjamin Herold
Staff Writer, Education Week

Follow Ben on Twitter: @BenjaminBHerold
Attacking the K-12 Cybersecurity Challenge

Expert Presenters:

Doug Levin
President
EdTech Strategies LLC

Melissa Tebbenkamp
Director of Instructional Technology
Raytown Quality Schools, Raytown, Mo.
An on-demand archive of this webinar will be available at www.edweek.org/go/webinar in less than 24 hrs.
Attacking the K-12 Cybersecurity Challenge: The Threat Landscape

Doug Levin | The K-12 Cybersecurity Resource Center
Defining Terms

cybersecurity **noun**
cy-ber-se-cur-i-ty \ ˈsī-bar-sē-, kyōr-ə-tē

**Definition of Cybersecurity**
- measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

**As distinguished from:**
- Internet safety
- Cyberbullying
- Digital citizenship
- School (physical) safety
- Student data privacy
The K-12 Cybersecurity Threat Landscape?
The K-12 Cyber Incident Map

Available online at k12cybersecure.com

Follow @K12CyberMap on Twitter—and sign up for the newsletter—for updates.
The K-12 Cyber Incident Map

442+ publicly-disclosed school cyber incidents since 2016

- Phishing attacks (blue)
- Data breaches (purple)
- Ransomware attacks (yellow)
- Denial-of-service attacks (green)
- Other incidents (red)

Available online at k12cybersecure.com

Follow @K12CyberMap on Twitter—and sign up for the newsletter—for updates.
The K-12 Cyber Incident Map

- Total number of incidents:
  - 2016: 67
  - 2017: 219
  - 2018: 122
  - 2019: 34 (so far...)

- 3 new K-12 incidents disclosed per week since 2016

- 7 percent of incidents are ‘repeat incidents’ (involving the same school district more than once)

Available online at k12cybersecure.com

Follow @K12CyberMap on Twitter—and sign up for the newsletter—for updates.
The K-12 Threat Landscape

1/ Which types of school districts are at risk?

2/ What types of incidents do districts experience?

3/ How significant are K-12 cybersecurity risks?
Which School Districts are at Risk?

Community Type:
- A - City: 23.77%
- B - Suburban: 37.47%
- C - Town: 15.5%
- D - Rural: 15.5%

Enrollment Size:
- A - Less than 1,000: 18.35%
- B - 1,000 - 2,499: 17.05%
- C - 2,500 - 9,999: 16.02%
- D - 10,000 - 24,999: 12.92%
- E - 25,000 - 99,999: 32.04%
- F - 100,000 or more: 3.62%

Poverty Status:
- A - Less than 10 percent: 27.63%
- B - 10 to 19.99 percent: 24.74%
- C - 20 to 29.99 percent: 35.53%
- D - 30 percent or more: 12.11%

Region:
- A - Northeast: 42.89%
- B - Southeast: 17.83%
- C - Central: 19.12%
- D - West: 17.83%
What Types of Incidents Do School Districts Experience?

- A - Denial of Service: 18.26%
- B - Phishing: 18.04%
- C - Ransomware: 18.95%
- D - Unauthorized Disclosure/Breach: 40.18%
- E - Other Incident: 4.57%
Illustrative K-12 Cyber Incidents

The ‘Top 10’ K-12 Cyber Incidents of 2018

During calendar year 2018, the K-12 Cyber Incident Map cataloged 122 publicly-disclosed cybersecurity incidents affecting 119 public K-12 education agencies across 38 states. What are the nature of these incidents? What is their real world impact? The ‘Top 10’ incidents of 2018 offer important insights.
‘Top 10’ K-12 Cyber Incidents of 2018

- In PA, Data Breach Puts Every Teacher in the State at Risk (Feb)
- Targeted Phishing Attack Leads to Identity Theft, Tax Fraud (Mar)
- Data Breach at Florida Virtual School Leads to Sale of Student Data on Dark Web (Mar)
- School District Pays $10,000 Bitcoin Ransom to Restore Access to Critical Systems (Apr)
- Police Raid Student’s Home in Grade Changing Incident (May)
- The FBI Warns of the Security, Privacy Risks of EdTech Adoption (Sept)
- U.S. Senator Calls for Federal Aid after School Networks Targeted (Oct)
- Disgruntled Former Employee Steals Sensitive District Database (Nov)
- TX District Scammed out of $2 Million School Construction Payment (Nov)
- On Cusp of Winter Break, District Discloses Massive Data Breach (Dec)

Learn more: https://k12cybersecure.com/year-in-review/2018-incidents/
Why are School Districts at Risk?

The motivations of perpetrators are varied:

- To steal money from schools (or from those affiliated with schools)
- To steal the identify of those who work in or attend schools
- To re-direct school IT assets toward other ends
- To make a political/policy statement
- To disrupt school operations
- To gain a personal advantage/to act on a grudge
- Because school staff and vendors/partners make mistakes
Resources

The K-12 Cybersecurity Resource Center
https://k12cybersecure.com

- K-12 Cyber Incident Map
- Semi-monthly newsletter
- Speaking schedule
- Research, resources, news, and commentary...
### Microsoft Secure Score

**Total score: 248 / 697**

Microsoft Secure Score analyzes the protection state of your identities, data, devices, apps, and infrastructure.

<table>
<thead>
<tr>
<th>Category</th>
<th>Score (Out of 100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>77 / 224</td>
</tr>
<tr>
<td>Protection state of your Azure AD accounts and roles</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>70 / 128</td>
</tr>
<tr>
<td>Protection state of your Office 365 documents</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>31 / 225</td>
</tr>
<tr>
<td>Protection state of your devices</td>
<td></td>
</tr>
<tr>
<td>App</td>
<td>70 / 120</td>
</tr>
<tr>
<td>Protection state of your email and cloud apps</td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td>(No data available)</td>
</tr>
<tr>
<td>Protection state of your Azure resources</td>
<td></td>
</tr>
</tbody>
</table>

#### History

- **13 points** in 30 days

- Your secure score over time and how you compare to other organizations.

#### URLs

- Microsoft Secure Score: [https://securescore.office.com](https://securescore.office.com)
- Cyber Defense: [https://aka.ms/edu/CyberDefense](https://aka.ms/edu/CyberDefense)
Melissa Tebbenkamp
Director of Instructional Technology
Raytown Quality Schools, MO
Data Governance

- Policy
- Data Stewardship
- Practice
- Security
- Procedure
- Data Privacy
Data Lifecycle

1. Identify Need
2. Create/Acquire
3. Manage/Store
4. Protect
5. Use/Share
6. Archive
7. Destroy
Network Stuff

- Firewall
- Content Filter
- Network Monitoring
- Partnership with ISP (DDOS)
- Segmented Networks (VLANs)
- Wireless network security
- Cyber Insurance (Data Breach)
Device Security

- Antivirus / Malware
- Restricted Access - no administrative access
- Updates / Patches
- Control applications
- Cyber Malpractice Insurance
Applications

- Contracts
- Role-based permissions
- Vet cloud-based applications
- Establish district approval process
- State, Local and Federal Regulations
- Insurance
  - Cloud-based vendors should protect you from breach
Humans make decisions based on knowledge and motivation.
Train, Train, Train

- Frequent
- Relevant
- Engaging
- Vary Delivery

- Students, Teachers, Admins, Board
National Effort

- Consortium for School Networking (COSN)
  - Protecting Privacy in Connected Learning
  - CyberSecurity
- Future of Privacy Forum (FPF)
- ED.gov Privacy Technical Assistance Center (PTAC)
Microsoft Threat Protection

Put an end to account compromise from phishing attacks

https://aka.ms/edu/CyberDefense
Microsoft Threat Protection

Protect – Detect - Respond
Take the sting out of ransomware.

https://aka.ms/edu/CyberDefense
An on-demand archive of this webinar will be available at www.edweek.org/go/webinar in less than 24 hrs.
Suggested Reading from *Education Week*:

**Special Report**

*K-12 Cybersecurity: Big Threats and Best Practices*

This *Education Week* examination of K-12 cybersecurity is the second of three special reports focused on the needs of K-12 district technology leaders, including chief technology officers.