OOPS!

SOMEONE JUST RAN A RED LIGHT.

Even the best cybersecurity tools can't stop human mistakes.

Have you ever mistakenly driven straight through an intersection controlled by a red stoplight?

We all make mistakes. It happens, despite the best of intentions.

It's the same situation for our information technology (IT) systems. Sometimes we mistakenly break the rules. So, we now find ourselves having to make policy surrounding cybersecurity – the science and information technology controls focused on keeping you, your computers, data, networks and electronic devices safe.

Inadvertent mistakes along our information highways – speeding through an IT red light – can jeopardize our safety.

Safety from what?

Safety from school shutdowns, ransoms, denial-of-service attacks, data theft, lawsuits, employee grievances, bullying, embarrassment and plain-old mischief.

It's hard to believe, but 90% of data breaches derive from phishing attacks, and "that's not a typo," says Cisco, the technology company who reported the figure in its 2021 report Cyber Security Threat Trends.[1]

By now, you are familiar with the term "phishing," the criminal seduction of computer users to act on malicious links or to divulge private information such as passwords, credentials or account numbers. Imposters and hackers are so good at their deceit that they have felled the mighty and the small by phishing.

Recall the CBS News report how the powerful John Podesta, chairman of the Democrats' 2016 presidential campaign, was victimized by a phishing scheme, but only after he correctly inquired about the validity of his suspicious email. In that case, Podesta obediently stopped at a red-light signal, but he got a green light from his IT helpers. "The Clinton campaign's own computer help desk thought it was a real email sent by Google," CBS News reported.[2] Podesta's emails became public.

Also, consider that behind the recent, wild rash of well-publicized ransomware attacks are hacker penetrations initiated through phishing schemes. Users mistakenly ran through the metaphorical stop sign. Once granted access behind the curtain of credentials, hackers began diagnostics and manipulations that lasted months before detection – a process called lateral movement. This advanced methodology distinguishes modern hacking from simplistic intrusions of the past.

CrowdStrike, a major cybersecurity company, defines lateral movement as "the techniques that a cyber attacker uses after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools."[3]

Kevin Mitnick knew how to disguise stop signs in front of his victims. He was a notorious hacker, focusing on the manipulation of phone systems predating today's computing infrastructure. His hardware and software hacking could not have been successful without what he called "social engineering." In his book *Ghosting the Wires*, Mitnick defined "social engineering" as the "casual or calculated manipulation of people to influence them to do things they would not ordinarily do. And convincing them without raising the least hint of suspicion."[4]

The results of this type of social engineering and subsequent cyber manipulation can be catastrophic. In Ohio, a 23,000-student district found data from its systems posted on a hacker's website. The stolen data included Social Security numbers, dates of birth, disability information on students and employee evaluations, according to the *Wall Street Journal*.[5]

In its investigations, the newspaper has also documented nearly 36 ransomware attacks against school districts during the COVID-19 pandemic going back to March of 2020. In seven cases, the *Journal* documented ransom payments of at least $2 million by school districts, colleges and universities.

In one case where a ransom was paid, a district still found 10% of its data inaccessible.

So, the No. 1 way school districts can curb cyber intrusions – to reduce that 90% number – is through training targeted to all employees and computer users within your agency. And on top of that, provide frequent reminders and enforcement.

Under such guidance, users will quickly develop habits that put the brakes on clicks for obvious phishing links. Still, other hacking tactics and social engineering strategies are less evident to everyday online computer users. Think about these potential scenarios where all the stop signs are missing, hidden or ignored:

- Busy employees delayed auto-updates to their computers' operating systems.
- A group of employees gathered for a late-afternoon meeting at a coffee shop where they used their district laptops to log in through an unsecured, public Wi-Fi network.
- An IT employee went to lunch but left the server room door unlocked while an open session was live onscreen.
- Security cameras in a board room were placed on a rear wall with a view of members' screens and keyboards; keystrokes were observable and recorded.
- On a trip to a conference, an administrator used a hotel network but failed to log in through the district's virtual private network.
- A parent at a reception counter memorized the keystrokes as a school secretary logged in to the school computer to start the day.
- A graphic arts teacher used the same username and password for school access as was used to download fonts on a free-font website.
- A rogue employee installed software to use laptop cameras to spy on students.

To counteract these cyber traffic violations, your IT department has numerous behind-the-scenes prevention tools. They are not so much red-light signals for users as they are police barriers, fences, warning cones, traffic cameras, sirens and the software akin to puncture strips used to stop high-speed-chase drivers.

In the technology world, laypeople are familiar with common tools such as antivirus software, email filters and firewalls, but lesser known to us are sophisticated tools such as packet sniffers, web gateways, port ID and traffic analysis monitors, and extended detection and response software – all used behind the curtain by IT staff.

Security software and consulting are now consuming a huge portion of IT budgets. PEPPM, the Pennsylvania-based purchasing cooperative, offers more than 400 already-bid purchasing contracts to simplify purchasing for IT professionals. Of those competitively bid PEPPM contracts, more than 15% are specifically related to some aspect of security, not counting other major network and computing brands that have cybersecurity built into their product offerings.

Every time a vendor or product is successful in shutting down a frequently mutating cyber threat, criminal hackers find new backdoors and ports to steal and vandalize. It's a war fueled by greed, power and ego. After you have done all you can to train employees to obey the red lights and warning signs, hackers will take the more difficult route on the information highway to get you. The ramp into your systems may come from third-party software and even your most-trusted enterprise tools. In these cases, you have little defense, and your agency is an unwitting victim.

The SolarWinds hacking is an example. SolarWinds is a highly respected provider of powerful and affordable IT management software with a variety of modules. It provides services to private companies, the federal government and even schools. Last year, the company was the target of Russian hackers (allegedly) who burgled into SolarWinds' systems and added malicious code into the company's software. It resulted in one of the "most sophisticated hacking campaigns ever conducted against the federal government," according to the federal Government Accountability Office.[6]

When the company sent out updates of its Orion production software (this particular software keeps watch over all the various components within an organization's network), the hackers' code planted trojans into the systems of SolarWinds clients. It forced the Department of Homeland Security to issue directives on how to mitigate the intrusion to federal agencies, including victimized Departments of Justice, Defense, Treasury and Energy.

With threats like these looming darker than ever, much of the current research and development in cybersecurity is targeted toward threat detection, threat hunters and threat monitoring. Products from these efforts are distinct from preventative types of software. Instead, they detect intrusions, hidden codes, trojans and file activity that may have already slipped past an agency's prevention tools and the users who sped through cyber stop signs.

These new kinds of threat-detection tools are valuable because new trojans and tactics are being forged constantly by highly trained actors (some sponsored by foreign governments). Then their creations — as in the case of SolarWinds – linger deep within your systems for months, patiently waiting for the ripe moment to launch a strike.

As cybersecurity evolves, some key policy decisions stand ready for school board members and administrators to appraise as they seek defenses to keep internal traffic and data safe:

1. Implement an ongoing communication strategy that alerts employees and computer users to social engineering traps and ensures they step on the brakes at first-level threats. A good communication strategy does not simply repeat the same "do-not" message over and over. Instead, attention-getting tactics include content that is newsworthy, peppered with funny and entertaining messages, and loaded with personal benefits for users.
2. Calculate the value of cybersecurity insurance. Do not depend upon a weak rider on your existing policy coverages. No organization is safe 100% over all systems, all users and all data. Therefore, your insurance should cover liabilities for the disclosure of private information and for business downtime, forensics, errors and omissions, public relations for crisis management, theft of money, system repair and legal expenses.
3. Be generous with money and approvals when your administration and IT departments request funds for assistance from consultants and outside experts. In small organizations, administrators and IT directors often don't know where to start, but the first step is reaching out for help from associations, federal and state experts and private consultants.

4. Encourage your IT, purchasing and administrative staff to use purchasing contracts for products that are already competitively bid by a trusted purchasing cooperative. That way, you save money from Day One, and there is no 30- to 60-day waiting period to buy and implement solutions that are needed to strengthen weak systems. Ransomware hackers are not stopping at any of your posted red lights. They could strike a vulnerable network tonight.
5. Mandate continuous professional development for your key IT personnel. Now is not the time to scrimp on conferences, certification courses, daily reading and networking. There's no better comfort being able to trust a well-trained IT professional just down the hall.

Above all, these and other well-crafted board policies on cybersecurity will clear the brush around your posted stop signs, keep power flowing to the red-light signals and position software cybercops for the quick cuffing of intruders.

Notes:

[1] *"2021 Cybersecurity Threat Trends: Phishing, Crypto Top the List": https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list*

[2] *An image of the actual email used to deceive John Podesta and his organization is posted in the CBS News report at https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/*

[3] *https://www.crowdstrike.com/cybersecurity-101/lateral-movement/*

[4] *Mitnick, Kevin. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Little, Brown and Company.*

[5] *"Schools Struggling to Stay Open Get Hit by Ransomware Attacks": https://www.wsj.com/articles/my-information-is-out-there-hackers-escalate-ransomware-attacks-on-schools-11605279160*

[6] *This website behind this link also provides an infographic timeline chronicling the discovery of the threat to SolarWinds and mitigating responses: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic*

PSBA
Pennsylvania School Boards Association