



BUILDING A CYBERSECURITY BLUEPRINT





PRESENTERS



MARCIA KAPLAN, CO-FOUNDER



STEVE KELLEY, CO-FOUNDER



JEFF BAJGOT, IT SECURITY CONSULTANT





Why Do You Need a Cybersecurity Blueprint?





EDUCATIONAL INSTITUTIONS ARE MORE THAN

2x

AS LIKELY TO BE TARGETED BY AN EMAIL COMPROMISE THAN OTHER ORGANIZATIONS.





IN ALMOST

90%

OF EMAIL ATTACKS AGAINST
SCHOOLS, THE CRIMINALS USED
GMAIL ACCOUNTS TO SEND THEIR
PHISHING EMAILS.

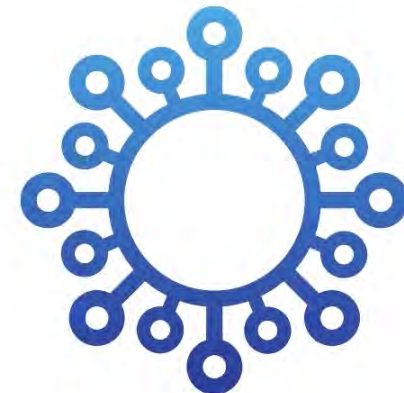




**A LARGE PERCENTAGE OF THE EMAILS
EXPLOITED**

COVID-19

**WITH SUCH SUBJECT LINES AS
"COVID19 NEW UPDATES," "COVID-19
UPDATE FOLLOW UP RIGHT NOW,"
"COVID-19 SCHOOL MEETING," AND
"RE: STAY SAFE."**

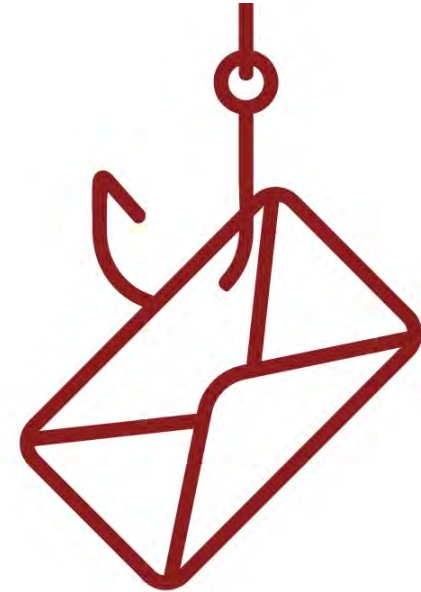




FROM JUNE THROUGH SEPTEMBER
2020, MORE THAN

1,000

EDUCATIONAL INSTITUTIONS
WERE TARGETS OF SPEAR PHISHING.



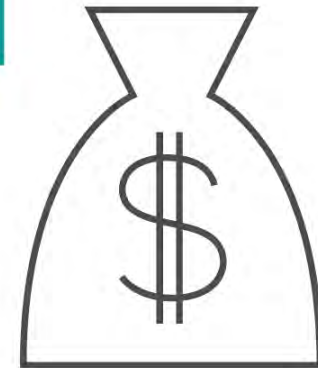


MANOR INDEPENDENT SCHOOL DISTRICT IN TEXAS LOST

\$2.3 million

DUE TO A FRAUDULENT PHISHING CAMPAIGN.

SCOTT COUNTY SCHOOLS IN KENTUCKY WAS TEMPORARILY SCAMMED OUT OF \$3.7 MILLION AS THE RESULT OF WIRE FRAUD.





TODAY'S K-12 CYBERSECURITY LANDSCAPE

K-12 lags behind most industries when it comes to cybersecurity.

Districts are struggling to find, hire, and retain qualified cybersecurity staff.

There is a growing awareness of the need for a formal K-12 Cybersecurity Plan to be developed and implemented.

K-12 tech leadership is beginning to shift budgets to support cybersecurity.





TODAY'S K-12 CYBERSECURITY LANDSCAPE

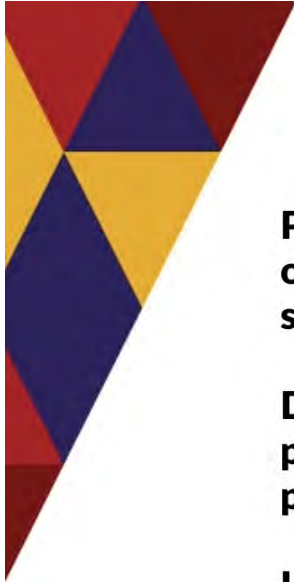
Schools are storing protected data in the Cloud/SaaS, relying on the due diligence and oversight of their suppliers.

Education leadership and school committees are beginning to seek timely information regarding cybersecurity.

Compliance to data privacy and protection regulations is an ever increasing concern.

Insurance companies are adding cyber insurance options; cost depends on risk factors, but schools do not do any assessment.





POTENTIAL RISKS

Phishing e-mails are the predominate risk for most organizations. They are becoming increasingly sophisticated and require new solutions.

Distributed Denials of Service (DDoS) attacks can paralyze your network. Most schools lack any preparation to combat DDoS.

Internet of Things (IoT) and network devices (e.g., IP security cameras) are being targeted by hackers and nefarious actors.





POTENTIAL RISKS

Patching and updating is lagging, creating an environment for hackers to exploit.

Advanced identity management solutions (e.g., password-protection software) and two-factor authentication are missing on critical information systems.

Encryption is used inconsistently.

Lack of enforcement in decommissioning users and devices.



IMPACT

4,000 ransomware attacks occur daily across the U.S.

Cybercriminals have encrypted systems, forcing schools to close or suspend remote learning until the ransom has been paid.

Cybercrime damages expected to reach \$6 trillion dollars this year.





K12 IT LEADERS' COMMON CONCERNS

A recent survey asked 300 K-12 edtech leaders about their top cybersecurity areas of need. Their responses:

- Need to create and follow a cybersecurity plan.**
- Real-time monitoring of cybersecurity events with incident response.**
- Understanding of cybersecurity investment ROI and third-party audits.**
- Continued employee training and stronger password policies.**
- Need for affordable access to cybersecurity resources when needed.**



7 COMMON MISCONCEPTIONS

- 1. We can manage cybersecurity with our existing resources.**
- 2. Cybersecurity is less of a priority because we use Apple and Google.**
- 3. Network management and cybersecurity management are the same thing.**
- 4. We have a fixed budget so we can't afford to invest in cybersecurity.**
- 5. Creating a Security Operations Center and leveraging cybersecurity threat intelligence is overkill and unaffordable.**
- 6. Cybersecurity crisis management is the responsibility of the Tech Director.**
- 7. We will not get hit with ransomware because we have good end-point protection and a firewall.**

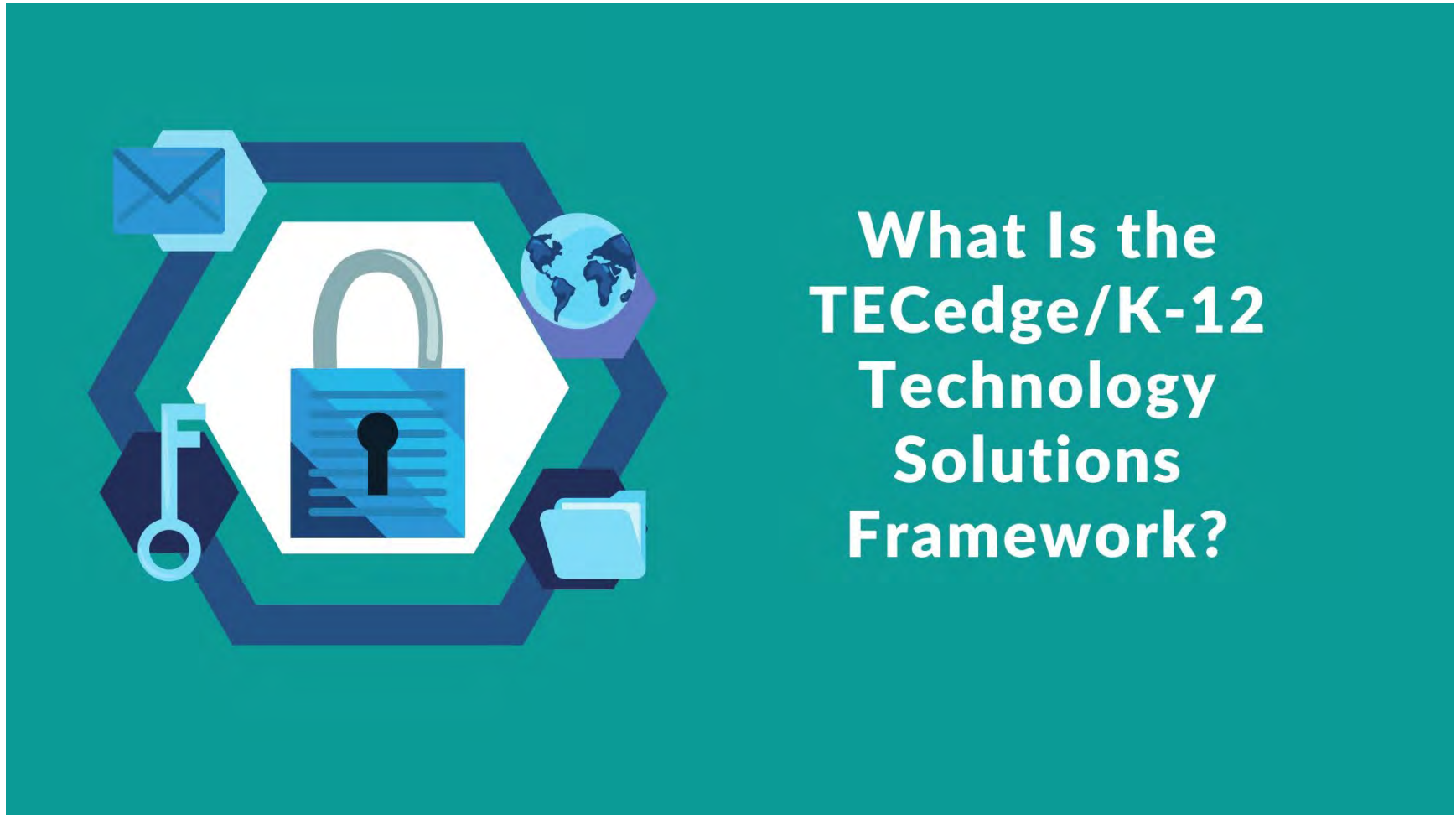




K-12 CYBERSECURITY CHALLENGES

- ✓ **Most districts have not performed a cybersecurity assessment.**
- ✓ **Most districts do not have a cybersecurity plan.**
- ✓ **It is unlikely that school IT budgets will be increased to address cybersecurity funding.**
- ✓ **Most districts do not have experienced cybersecurity staff.**
- ✓ **Schools will be spending what money they have for cybersecurity without a plan.**
- ✓ **Additional funding will be needed to address the challenge.**







CYBERSECURITY GOVERNANCE GOALS



- What do we have that needs protecting?
- Where do we have it?
- How do we provide protection?
- What should we do if there is an incident?





CYBERSECURITY ASSESSMENT FOUNDATION

Use the standards recommended in the U.S. Department of Homeland Security’s Catalog of Control Systems Security: Recommendations for Standards Developers.






The development team consisted of representatives from the National Institute of Standards and Technology (NIST) & the Department of Energy National Laboratories.





LEVERAGE NIST CYBERSECURITY FRAMEWORK

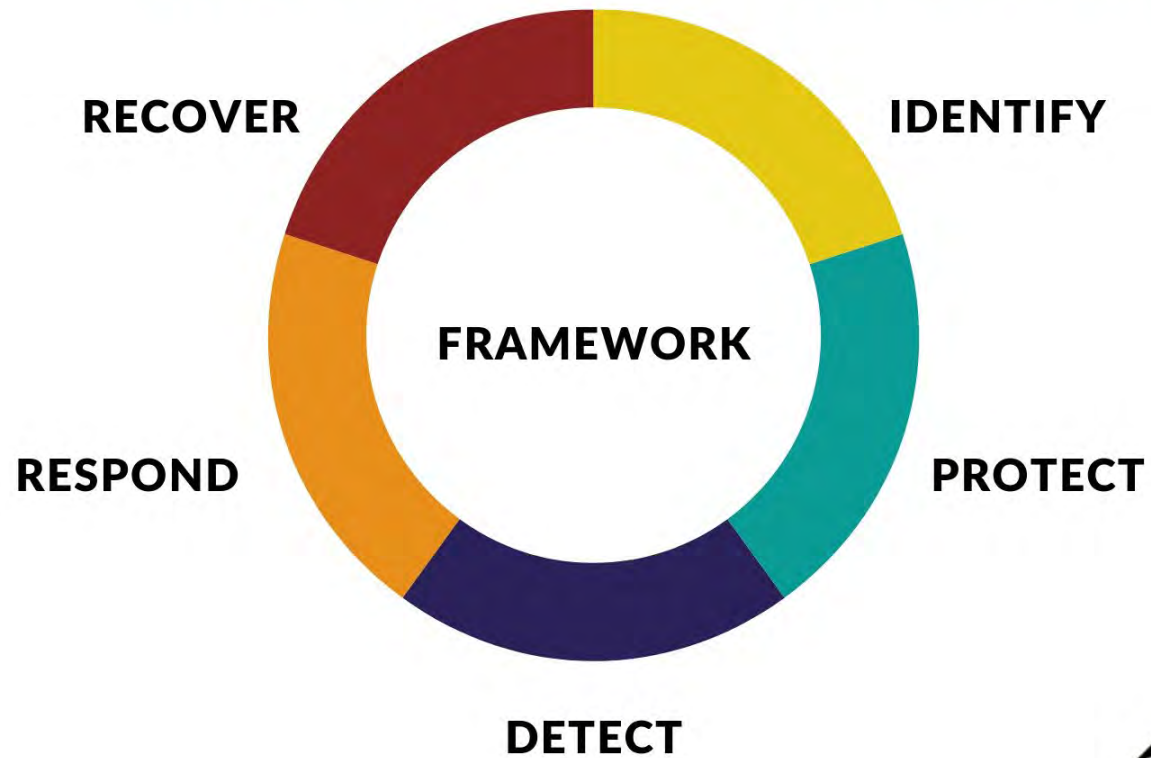
The NIST Framework provides a common taxonomy and mechanism for organizations to:

-  Describe their current cybersecurity posture
-  Describe their target state for cybersecurity
-  Identify and prioritize opportunities for improvement within the context of a continuous and repeatable processes
-  Assess progress toward the target state
-  Communicate among internal and external stakeholders about cybersecurity risk





NIST CYBERSECURITY FRAMEWORK





NIST CYBERSECURITY FRAMEWORK

- Identify.** Understand how to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect.** Develop safeguards to delivery critical infrastructure services.
- Detect.** Implement the activities to identify a cybersecurity event.
- Respond.** Identify how to take action regarding a detected cybersecurity event.
- Recover.** Develop how to maintain plans for resilience and to restore any capabilities or services that were impaired.







SETTING UP A HIGHLY FUNCTIONAL CYBERSECURITY TEAM

- ✓ **Expectations**
- ✓ **Roles & Responsibilities**
- ✓ **Time Commitment**
- ✓ **Organizational Structure**



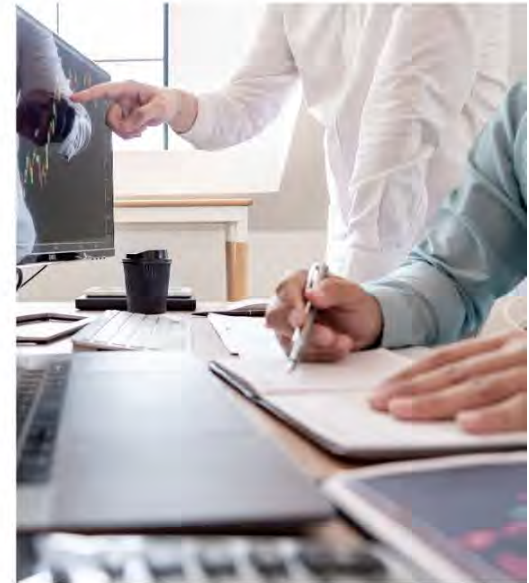


CYBER RISK MANAGEMENT

Risk management is the job of district leadership in partnership with IT.

Questions to ask your IT manager:

- How many significant cyber incidents has the district experienced?**
- How do we measure our cybersecurity program's effectiveness?**
- How much of our IT budget is being spent on cybersecurity-related activities?**
- What metrics do we use to evaluate cybersecurity awareness?**





K-12 CYBERSECURITY BLUEPRINT PROCESS

Conduct an assessment of existing cybersecurity posture.

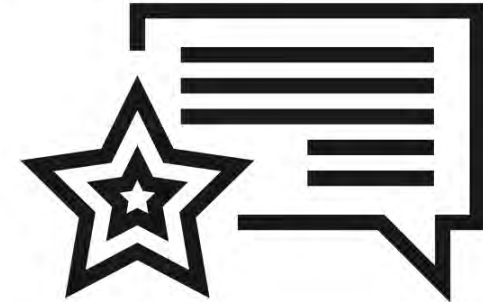
Create key findings outlining your organization’s cybersecurity risks and vulnerabilities.

Recommend areas and strategies to mitigate and reduce risk.

Develop prioritized set of recommendations with preliminary budget.

Present Cybersecurity Blueprint to stakeholders.

Provide 90-day review and update.





TOOL FOR ASSESSING CYBERSECURITY ACTIVITIES

Leverage the TECedge/K-12 Technology Solutions customized version of the Cyber Security Evaluation Tool (CSET).

CSET was developed by Homeland Security’s Cybersecurity & Infrastructure Security Agency (CISA).

The K-12 customized CSET Tool provides a systematic, disciplined, repeatable approach for evaluating an organization’s security posture.





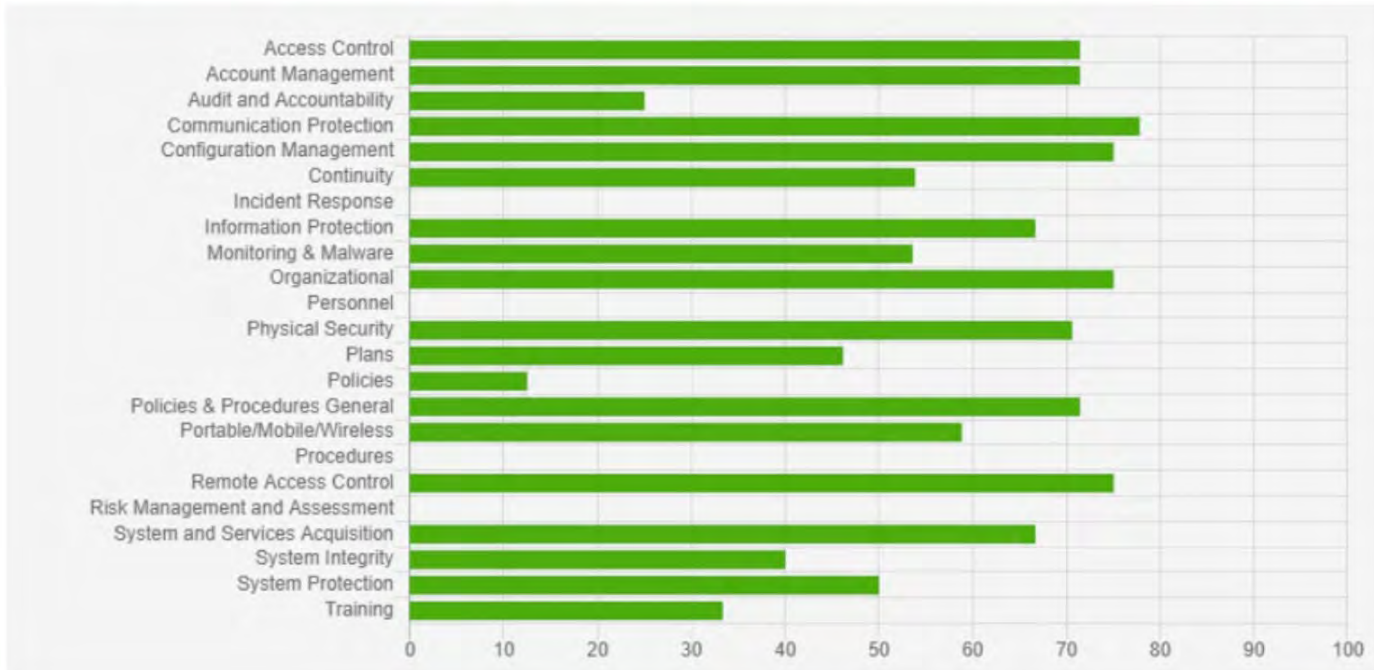
DATA COLLECTION

- Identify focus group participants & key stakeholders.**
- Provide key stakeholders with NIST questions.**
- Interview key stakeholders.**
- Conduct in-depth interviews with stakeholders using the CSET Tool.**
- Enter each stakeholder's responses into CSET.**
- Generate findings and recommendations.**





SAMPLE BLUEPRINT ASSESSMENT CHART





CYBERSECURITY ASSESSMENT & PLAN

Introduction & Background

Study Methodology

NIST Framework:

- Identify
- Protect
- Detect
- Respond
- Recover

Planning

- Define cyber staff roles and responsibilities
- Develop cybersecurity policies and procedures
- Develop implementation plan
- Train staff, educators, and students



WHAT DIFFERENTIATES US?



Proven planning & assessment process from 30 years of experience

Vendor independent

Ability to align the needs of K-12 education with NIST cybersecurity standards





For more information, please contact:

Marcia Kaplan
mkaplan@tecedge.net
617-276-6478
www.tecedge.net

Jeffrey M. Bajgot
bajgot@k12-technology.com
508-657-4495
www.k12-technology.com



