WORKFORCE DEVELOPMENT COMMITTEE STRATEGIC PLAN

Chair: Commissioner Fred Payne
Co-Chair: Dr. John Keller

October 2021
Indiana Executive Council on Cybersecurity

Workforce Development Committee Plan

Table of Contents

Committee Members

Committee Members

Last Name	First Name	Organization	Organizational Title	Member Type (Chair/Co-chair/Full-time, As needed)
Akgul	Arif	Indiana State University	Assistant Professor - School of Criminology & Security Studies	Full Time
Bailey	George	Purdue University / cyberTAP	Assistant Director, cyberTAP / Professional Services	As Needed
Cloud	Matthew	Ivy Tech Community College of Indiana-Lake County Campus	Director of Cybersecurity Grants, Asst. Prof. of Data Analytics, and Dept. Chair School of IT and Criminal Justice	As Needed
Frank	Michael	Anderson University	Professor of Political Science	Full Time
Jirik	Jiri	Ivy Tech Community College	Assistant Professor - Evansville	As Needed
Keller	John (Dr.)	Indiana Department of Education	Chief Information Officer, IT	Co-chair
Knies	John	Lumen	Director Information Security	As Needed
Koressel	Jake	Indiana Department of Education	Computer Science Specialist	Full Time
Korty	Andrew	Indiana University	Chief Information Security Officer	Full Time
Lubbers	Teresa	Indiana Commission for Higher Education	Commissioner	As Needed
Mathis	Dan	Indiana Office of Technology	Compliance Manger	As Needed
Meadors	Joe	Gaylor Electric Inc	Vice President of Information Services	As Needed
Neely	Dewand	MGT Consulting	Chief Information Officer	Full Time
Odum	Matt	Briljent, LLC	President	As Needed
Payne	Fred	Indiana Department of Workforce Development	Commissioner	Chair
Rapp	Douglas	Cyber Leadership Alliance	President	Full Time
Salahieh	Rami Maximus	Ivy Tech Community College, Valparaiso, NIISSA	CSIA Program Chair, CSOC Valpo Director	Full Time

Scarbro Kennedy	Valinda	IBM	IBM Global University Specialty Programs Manager-Medical, Legal, and HBCUs	Full Time
Schmelz	Pam	Ivy Tech Community College	Chair, School of Information Technology	Full Time
Shemroske	Ken	University of Southern Indiana	Associate Professor of Computer Information Systems	Full Time
Tucker	Jeff	Indiana Department of Workforce Development	Chief Information Officer	Chair Proxy
Rogers	Marc	Purdue University	Executive Director, Purdue Cyber Apprenticeship Program, and Clinical Professor	Full Time
Vespa	Tony	Vespa Group, LLC	Owner	As Needed
Downes	LeighAnne	Indiana Department of Workforce Development	Technology Liaison Sr	As Needed

Introduction

Introduction

The world of cybersecurity is highly complex and cluttered with information, misinformation, and disinformation. As a consequence, it is important to approach it strategically and create simplicity.

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) continues its mission to move efforts and statewide cybersecurity initiatives to the “Next Level.” With the ever-growing threat of cyberattacks, protecting Indiana’s critical infrastructure is the focus of the IECC. Cybersecurity cannot be solved by one entity alone. The IECC works with private, public, academic, and military partners from all over the state to develop and maintain a strategic framework that establishes goals, plans, and best practices for cybersecurity.

The IECC is comprised of fifteen committees and working groups who have worked together to implement the statewide strategy of 2018 while developing an updated comprehensive strategic plan.

The following implementation plan is one of the fifteen specific plans that encompass the complete *2021 Indiana Cybersecurity Strategic Plan*.

For more information, visit www.in.gov/cybersecurity.

Executive Summary

Executive Summary

- **Research Conducted**
  - Searched for:
    - Review of previous committee deliverables for updates and re-use.
    - Validate and complete list of all cybersecurity courses/programs/degrees/etc.
    - Source for current and future demand for cybersecurity workers in Indiana
    - List of all cybersecurity-related jobs and the skills required to fill those jobs
    - Info on how easy/difficult it is to fill cybersecurity jobs, currently
    - List of programs designed to generate interest in cybersecurity and a career in cybersecurity
    - What has happened in the recent past in this area in Indiana
    - Existing data on cybersecurity programs/courses/degrees/certifications and the capability of that data

- **Research Findings**
  - It is difficult, in most cases, to quickly fill cybersecurity-related jobs with people who have the required skills
  - It is difficult to understand all the training opportunities available to Indiana's labor force and talent pipeline
  - The National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) has developed a Cybersecurity Workforce Framework. This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework is being reviewed by other states and has been widely adopted.
  - There are many existing and effective programs to generate interest in cybersecurity, measure aptitude, provide needed skills and/or certifications, etc. This committee's initial efforts on many of our deliverables will be to develop effective ways to leverage these existing initiatives before trying to create something new.
  - There are other closely related programs to which cybersecurity content could be added to further promote the field of cybersecurity and generate interest.
  - Existing data on cybersecurity programs/courses/degrees/certifications may not be up to date enough to satisfy all our committee goals.

- **Committee Deliverables**
  - Enhance CyberseekIN.org Data Tool
  - Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard
  - Update K-12 Cybersecurity Content
  - Promote cybersecurity training across the K-12 sector to protect the educational process
  - Update the CHE Cyber Program Data Tool and Report

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity**?
    a. Inventoried cyber related course offerings available within Indiana's higher education network so we have a better understanding our education pipeline.

2. **What (or who) are the most significant cyber vulnerabilities in your area?**
    a. Near-term challenge – a shortage of people with needed skills to fill open cybersecurity positions. The longer-term challenge will be the strategic filling of the pipeline to ensure Indiana is well positioned not just to fill open cybersecurity positions, but to also provide a workforce that would aid in attracting cybersecurity firms to locate in Indiana.

3. **What is your area's greatest cybersecurity need and/or gap?**
    a. Biggest need continues to be people with cybersecurity skills to fill open cybersecurity jobs.

4. **What federal, state, or local cyber regulations is your area beholden to currently?**
    a. Not Applicable

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. From a workforce perspective, there is a Cybersecurity Workforce Framework that has been developed by the National Initiative for Cybersecurity Education (NICE) which is a part of National Institute of Standards and Technology (NIST). This framework provides a common language to be used to describe tasks, knowledge, skills, and abilities needed for each cybersecurity work role. This framework is now widely adopted by other states and tools are being developed to facilitate the implementation of the framework (e.g., a job description writing tool).
    b. Purdue's Cyber Apprenticeship Program, along with Indiana's Office of Work-Based Learning and Apprenticeships, offer an exciting way to connect interested talent with motivated employers.

6. **What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc.**
    a. Indiana has plenty of data about the current state of affairs at various levels of the cybersecurity pipeline including data from Indiana Department of Education (IDOE), Department of Workforce Development (DWD), and Commission for Higher Education (CHE). The IEDC Cyber Initiative report provided a starting point for many of our committee's initial deliverables: framework, program list, job demand challenges, etc.

7. **What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?**
    a. See answer to #5 above.
    b. Offering free cyber courseware online to students to promote awareness and interest of the cyber industry.

8. **What does success look like for your area in one year, three years, and five years?**
    a. Sufficient quantity of skilled workers to fill all cybersecurity positions.
    b. Ability to see current and future demand for all cybersecurity jobs.
    c. Ability to understand the skills associated with all jobs that make up the demand.
    d. Ability to see all students in the pipeline that are in programs that provide them the needed skills to fill that demand.
    e. A better alignment of activity in the K-12 system and the nurturing that needs to happen to progress from broad competencies in early grades to focused skills and proficiency as students move through high school and into college.

9. **What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?**
    a. This is what our committee is working on as part of the IECC.

10. **What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?**
    a. Due to limitations in how this data is gathered, an accurate number is difficult to determine. Anecdotal data suggests that there are not enough cybersecurity workers to fill all open positions. It is likely that in many cases, employers are filling these positions and providing or arranging for the appropriate training. A key deliverable for our team is to develop methods/models to identify the current and future demand for all cybersecurity jobs in Indiana – the types of cybersecurity jobs and the required skills. It is reasonably assumed that the need for cybersecurity-skilled workers will grow, and one specific need will be for K-12 instructors. This may provide an opportunity to look into the feasibility of engaging individuals with cybersecurity expertise as instructors even though they don't have teaching licenses.

11. **What do we need to do to attract cyber companies to Indiana?**
    a. The primary requirement from our committee's perspective - provide a capable and skilled workforce.

12. **What are your communication protocols in a cyber emergency?**
    a. Not Applicable

13. **What best practices should be used across the sectors in Indiana? Please collect and document.**
    a. National Initiative for Cybersecurity Education Cybersecurity Workforce Framework – provides a common language for all cybersecurity work roles and the tasks, knowledge, skills, and abilities needed for each.

Deliverable: Enhance CyberseekIN.org Data Tool

Deliverable: Enhance CyberseekIN.org Data Tool

General Information

1. **What is the deliverable?**
   a. Enhance CyberseekIN.org Data Tool

2. **What is the status of this deliverable?**
   ☐ Completed ☐ In-progress 25% ☒ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. Which of the following categories most closely aligns with this deliverable (check **ONE**)?
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group
   or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable:

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Continuously updating and adding new functionality to a “go to” site dedicated to Cybersecurity occupations/training for the State of Indiana helps to strengthen the focus on a growing industry sector for talent and employers.

6. **What metric or measurement will be used to define success?**
   a. Data analytics to monitor usage and length of site visit including page access as well as other “clicks” within the site to determine user movement.

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Job Seekers and Employers as well as other workforce development and training entities

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Some cybersecurity occupations/job postings/training options are visible in Indiana Career Connect and Indiana Career Ready sites operated by the Department of Workforce Development.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. No Response

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DWD is working with Burning Glass Technologies, Purdue University's PCAP program as well as a group of training providers and employers.

12. **Who should be main lead of this deliverable?**
    a. Department of Workforce Development – IT Department

13. **What are the expected challenges to completing this deliverable?**
    a. Because cybersecurity is an emerging occupation group, some national data links such as CIP & SOC codes as well as ONET data have not yet categorized occupations in this industry with their own set of identification codes – many occupations (under cybersecurity) are sharing industry codes with other industry sectors employing similar occupations.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**

☐ One-time deliverable

☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Integrate CyberseekIN with CHE's Credential Engine	DWD	0	June 2022	Need to understand CE roadmap and timelines
Refresh Training providers in Cyberseek	DWD	0	October 2022	Initial launch was a one-time feed of training providers

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1	1	Project Management	TBD	TBD	Staff and outside vendor to complete all edits

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Burning Glass Technologies	Hosting of site	$140,000 – development and site hosting costs	TBD	TBD	TBD	Site is part of DWD's 3 year contract with BGT

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. One stop shop for Cybersecurity job seekers, employers, and training provider information

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. The site will educate Hoosiers on the cyber security industry and what occupations are available relative to what education is needed to be successful.

19. What is the risk or cost of not completing this deliverable?

a. Not building an insource of talent to full fill the Indiana employers growing need for cybersecurity specific talent. Indiana is exposed to employers seeking talent outside of Indiana as well as locating any business growth opportunities to states/countries that can meet their growing need.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Data analytics can be added to the site to monitor traffic usage and length of stay

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

☐No ☒ Yes

a. Burning Glass Technologies built a national cyberseek.org site that is currently operational and linkable from the Indiana site. This site provides cybersecurity information nationally.

22. Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☐No ☒ Yes

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Budget: not having the funding to continue to host and enhance the site.

b. Resources: not having participation of training providers, employers and job seekers could negatively impact the validity of the site.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Currently, DWD is committed to providing data and resources as needed to continue the site data and hosting. Finding and securing funding is always a necessity.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. This deliverable is already built and launched.

27. Can this deliverable be used by other sectors?

☒No ☐ Yes

a. This site is specifically designed to enhance Indiana's presence in cybersecurity industry sector. Other business sectors do have access to this site and can use this site to fulfill their business needs for cybersecurity.

.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Site is fully operational and has been launched. There have been some communications released from DWD's Marketing and Communications group. Other opportunities to bring attention to the site is needed. DWD is open to participating with interested groups to further bring awareness to the tool.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

a. The tool currently links to the Indiana's cybersecurity website.

30. What are other public relations and/or marketing considerations to be noted?

a. The site was featured as part of the Indiana Chamber of Commerce cybersecurity forum held this past July 2021. So continued marketing such as this will need to be done through partners and associations.

Evaluation Methodology

Objective 1: Indiana DWD will add Credential Engine certifications data to CyberseekIN.org (training providers) by June 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana DWD continue Data enhancements to CyberSeekIN.org including continual updates to training providers, Apprenticeship Data/Opportunities, and Promote opportunities, training, events surrounding cybersecurity in Indiana by October 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard

Deliverable: Enhance Cybersecurity Talent Pipeline and Job Openings Dashboard

General Information

1. **What is the deliverable?**
   a. Cybersecurity Talent Pipeline and Job Openings Dashboard

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Create a dashboard measuring Indiana's job demand, talent pipeline, apprenticeships and training opportunities

6. **What metric or measurement will be used to define success?**
   a. Create a data collection tool to use for informational purpose to power the dashboard with the most up-to-date demand, pipeline as well as apprenticeships/training opportunities. Final measurement would be a published dashboard.

7. **What year will the deliverable be completed?**

   ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. Job Seekers, Training Providers, employers s

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Some cybersecurity occupations/job postings/training options are visible in Indiana Career Connect and Indiana Career Ready sites operated by the Department of Workforce Development.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None at this time.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. DWD would need to be involved based on the multiple avenues we currently have for data collection. Would also use DOE and Apprenticeship

12. **Who should be main lead of this deliverable?**
    a. Department of Workforce Development – IT Department

13. **What are the expected challenges to completing this deliverable**?
    a. Because cybersecurity is an emerging occupation important data codes may bridge across multiple industries.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**

    ☐ One-time deliverable

    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Analysis of current dashboard data sets and metrics	DWD	10	11/1/2021	
Analysis of potential data sets and how they could be incorporated into existing dashboards	DWD/BG	0	12/1/2021	
Implement changes to dashboard with cyberseek	BG	0	1/31/2022	May require contract amendment

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1	1	Research and Project Mgt	TBD	TBD	Staff and identified other resources

16. What other resources are required to complete this deliverable?

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
TBD						

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Help Indiana keep a pulse on a growing industry sector and show Hoosiers a growth pattern in cybersecurity.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. The site will educate Hoosiers on what cybersecurity opportunities are available and what training needs exist to support the roles.

19. What is the risk or cost of not completing this deliverable?

a. Not building an insource of talent to fulfill the Indiana employers growing need for cybersecurity specific talent. Indiana is exposed to employers seeking talent outside of Indiana as well as locating any business growth opportunities to states/countries that can meet their growing need.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Success would be defined as a completed dashboard that integrates real time data for cybersecurity employment and training provider information

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

a. Unknown at this time

22. Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Unknown at this time

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Budget: not having funding to follow through with development of a robust system
b. Resources: not having needed participation of training partners, employers and job seekers

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐ Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Partnerships with other agencies as well as outside companies support the data needed to power the dashboard can be researched, but creating partnerships is even more collaborative.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. DWD - IT

27. Can this deliverable be used by other sectors?

☐No ☒ Yes,

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Unknown

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Undetermined at this time.

Evaluation Methodology

Objective 1: Indiana Department of Workforce Develop create cybersecurity workforce dashboard metrics – measuring Indiana’s job demand, talent pipeline, apprenticeships, and training opportunities by January 2022.

Type: ☒ Output ☐ Outcome

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Update K-12 Cybersecurity Content

Deliverable: Update K-12 Cybersecurity Content

General Information

1. **What is the deliverable?**
   a. Develop and promote high school CTE programs of study.
   b. Increase the number of K-12 staff equipped to teach cybersecurity related courses and courses incorporation cybersecurity related content.

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50%. ☐ In-progress 75%. ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. In conjunction with the Governor’s Workforce Cabinet and the IDOE will support the development of high school Career and Technical Education programs of study in Cybersecurity and support efforts to increase awareness of such programs with students, families and parents. The IDOE’s support will include developing resources for instructors to help them deliver cybersecurity content to students in the courses and programs on this topic. IDOE will develop and curate professional development resources on cybersecurity across the K-12 continuum.

6. **What metric or measurement will be used to define success?**
    a. Number of programs statewide offering with verifiable alignment to cybersecurity concepts and content.
    b. Scope and sequence showing development/articulation of cybersecurity concepts across grades K-12.
    c. Increase in professional development for teachers at all levels.
    d. Number of individuals receiving industry credentials or certificates from completing cybersecurity classes (post-graduation)
    e. Number of individuals participating in educational and experiential programs

7. **What year will the deliverable be completed?**
    ☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. The workforce would be the ultimate beneficiary of this long-range development.
    b. Near-term, students would benefit from more opportunities for cybersecurity attainment.
    c. Underserved and underrepresented populations will be more evenly represented in STEM careers.
    d. Could also be some benefit of a more informed citizenry—from the more intentional inclusion of cybersecurity in the K-12 curriculum.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. State or Federal STEM/Computer science programming and funding opportunities.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Governor's Workforce Cabinet
    b. Professional development providers
    c. Commission for Higher Education

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. IDOE along with those who provide content/training for the proposed K-12 computer science offerings across the state.
    b. Governor's Workforce Cabinet (GWC)
    c. Commission for Higher Education

12. Who should be main lead of this deliverable?

a. IDOE/GWC

13. What are the expected challenges to completing this deliverable?

a. Ensuring that consistent (and correct) content is included in all the various offerings/programs statewide.
b. Training teachers
c. Identifying funding
d. Writing curriculum and balancing the proposed additions with other content areas vying for attention within the K-12 curriculum.
e. Statewide implementation

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

☐ One-time deliverable
☒ Ongoing/sustained effort

Tactic Timeline

Tactic	**Owner**	**% Complete**	**Deadline**	**Notes**
Include cybersecurity topics as part of ongoing computer science professional development for K-12 teachers.	IDOE	25	Fall 2023	This program of study is available for adoption by all Indiana High Schools.
Promote the development of a Cybersecurity program of study	GWC	100	Spring 2021	This content will be available through the Learning Lab (Digital platform sponsored by IDOE to distribute Professional Development) and on the IDOE web site.

Resources and Budget

15. Will staff be required to complete this deliverable?

☒No ☐ Yes

Estimated Initial FTE	**Estimated Continued FTE**	**Skillset/Role**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
None					

16. What other resources are required to complete this deliverable?

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Expert Consultation	Guidance and project management to develop Cybersecurity standards for K-12	TBD	TBD	State/Federal	Grants	

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Opportunities for high school students to earn workforce relevant cybersecurity skills and credentials with support from high quality instructors.

b. Opportunities for teachers to improve their instructional skills in the area of cybersecurity and computer science.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. This would reduce the cybersecurity risk or impact in two ways

i. Ensuring that all students receive basic exposure to cybersecurity content throughout their time in Indiana schools.

ii. Increasing the pool of available job seekers with relevant cybersecurity credentials.

19. What is the risk or cost of not completing this deliverable?

a. Lack of opportunities for Indiana students to receive relevant preparation for the workforce. May impact the competitive edge for Indiana if we must always import cybersecurity professionals to meet the growing demand.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Number of Indiana high school students earning industry recognized cybersecurity credentials.

b. Number of teachers available to meet demand for cybersecurity related courses.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

22. Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☐No ☒Yes

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Any results with direct impact to the economy are years away.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☒No ☐Yes

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Ongoing investment in this programming and ensuring its availability across schools and geographies.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. This deliverable is consistent with interagency plans being developed by the Governor's Workforce Cabinet, Indiana Department of Education, and Commission for Higher Education.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. Creating more potential job candidates would help any sector needing cybersecurity professionals and expertise.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana K-12 schools

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

None at the moment.

Evaluation Methodology

Objective 1: Governor's Workforce Cabinet with support from IDOE will develop and promote a high school CTE Program of Study in Cybersecurity by June 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Indiana Department of Education will develop a menu of cybersecurity-related professional development and resources, including K-12 computer science offerings, by June 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: Indiana Department of Education and Cybersecurity Program Director will edit and distribute the Cybersecurity for Education Toolkit 2.0 by February 2022.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Promote Cybersecurity Training Across the K-12 Sector to Protect the Educational Process

Deliverable: Promote cybersecurity training across the K-12 sector to protect the educational process

General Information

1. **What is the deliverable?**
   a. Proposal to ensure an appropriate level of cybersecurity content is included in K-12 computer science offerings (per the Governor's Next Level Plan) and other initiatives, as appropriate (e.g., Hour of Code). On the one hand, this deliverable could be as simple as adding a layer of coordination across existing initiatives. On the other hand, it could be as expansive as creating formal expectations about cybersecurity in the K-12 curriculum with clear connections between the knowledge and skills students should have, when they should have them, and how they can be obtained.
   b. Identify, map and vertically align cybersecurity curricula to state and national standards.
   c. Pilot and scale up IN Cyberpath programs for P-16 and other postsecondary programs to increase student content knowledge and experience in cybersecurity.
   d. Create access and opportunity for underserved and underrepresented populations
   e. Increase the number of individuals going into cybersecurity jobs

2. **What is the status of this deliverable?**
   ☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. **Which of the following IECC goals does this deliverable meet?**
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☐ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☒ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
   a. Ensures that Hoosiers get exposure to Cybersecurity concepts early. This knowledge will help them decide if they might be interested in pursuing further education and a career in cybersecurity. At a minimum, this makes people more aware of good cybersecurity practices that will benefit them their entire life. The concepts relevant to cybersecurity in the workforce should be mapped back to the K-12 curriculum including broadly relevant content at early grades that would provide foundational understandings, dispositions, and skill development necessary to more focused skill development at the middle and high school levels.

6. **What metric or measurement will be used to define success?**
   a. Number of programs statewide offering with verifiable alignment to cybersecurity concepts and content.
   b. Scope and sequence showing development/articulation of cybersecurity concepts across grades K-12.
   c. Increase in professional development for teachers at all levels.
   d. Development of computer science strategic plans by schools with particular emphasis on the growth and development of students with strong preparation in cybersecurity.
   e. Number of postsecondary courses stood up that allows individuals to receive badges or certificates for indicating course completion.
   f. Number of individuals receiving badges or certificates from completing cybersecurity classes (post-graduation)
   g. Number of individuals participating in educational and experiential programs

7. **What year will the deliverable be completed?**
   ☐ 2021 ☒ 2022 ☒ 2023 ☒ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
   a. The workforce would be the ultimate beneficiary of this long-range development.
   b. Near-term, students would benefit from more opportunities for science attainment.
   c. Underserved and underrepresented populations will be more evenly represented in STEM careers.
   d. Could also be some benefit of a more informed citizenry—from the more intentional inclusion of cybersecurity in the K-12 curriculum.

9. **Which state or federal resources or programs overlap with this deliverable?**
   a. Any funding targeting the development of STEM programming at the K-12 level.

Additional Questions

10. What other committees and/or working groups will your team be working with to complete or plan this deliverable?

a. No plans for work with other groups at the moment. This deliverable will require substantial vision and investment from policymakers and will take years to implement.

b. IN CyberPath via Purdue University and Indiana University

11. Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?

a. DOE along with those who provide content/training for the proposed K-12 computer science offerings across the state.

b. IN CyberPath Team

c. NICE

d. Burning Glass

e. Because of the scale of the work, there could be many contributors but there must be a goal, a shared vision, and an organization anointed to lead the charge.

12. Who should be main lead of this deliverable?

a. IDOE

b. IN CyberPath team

13. What are the expected challenges to completing this deliverable?

a. Ensuring that consistent (and correct) content is included in all of the various offerings/programs statewide.

b. Training teachers

c. Identifying funding

d. Writing curriculum and balancing the proposed additions with other content areas vying for attention within the K-12 curriculum.

e. Integrating cybersecurity curriculum into existing classroom practices

f. Statewide implementation

Implementation Plan

14. Is this a one-time deliverable or one that will require sustainability?

☐ One-time deliverable

☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Increase the number of schools certified through Common Sense Media to 200.	IDOE	80	Fall 2023	16-17 school year there were 167 Indiana Schools Certified (https://d1e2bohyu2u2w9.cloudfront.net/education/sites/default/files/certified_schools_16_17_final.pdf)
Develop K-12 appropriate emphasis for Cybersecurity Month in October	IDOE	0	October 2024	Could use the cybersecurity month as a platform for promoting an array of options for schools.
Develop an annotated curricular resources hub for K-12 teachers	IDOE	0	September 2024	This could be at least partially met through the new CyberSecurity programming to be launched by the IDOE.
Develop and implement IN CyberPath	IN CyberPath	0	2023	This is a three-phase program. Phase one includes focus groups and development of the cyberseek took for Indiana. Phase two implements pilot programs both K-12 and CareerMakers. Phase three rolls programs out full scale across state.
Identify links between the professional development Code.org is offering to Indiana teachers and the cybersecurity domain.	IDOE	0	September 2024	
Promote the development of a Cybersecurity Graduation Pathway	SBOE	0	2024	The State Board of Education has a process for reviewing Locally Created Pathways as part of the programming they are developing around Graduation Pathways.
Pilot Beta Offering of PLTW CyberSecurity course for 10th graders	IDOE	10	September 2024	IDOE to fund participation by up to 10 schools interested in piloting this course.
Pilot phishing simulations with students through the state procured platform (Media Pro)	IDOE	0	September 2024	IDOE is working to make the MediaPro platform available to all Indiana Schools. This platform includes access to a phishing simulation and training content.
Create and adopt a formal set of standards	IDOE	0	September 2024	This is a big lift but would really help to lay the foundation for moving from

for cybersecurity across the K-12 curriculum				the piecemeal approach we have now to a more full-court press, so all students have basic awareness and understanding about cybersecurity matters—a new essential skill to be an educated citizen.
Create cybersecurity summer camp for k-12 students.	IU	90	Summer 2023	Indiana University will run the Security Matters Cybercamp for interested students from throughout the state and use the workforce development subcommittee to help promote the camp.
Create CareerMaker course for post-secondary training, offering certificates and/or badges for completion.	IN CyberPath Team	0	2024	This is part of the IN CyberPath project with Purdue and IU

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
1.0	1.0	Management coordination, advocacy	State		There are bits and pieces of the tactics enumerated above that are already underway, what is needed is an individual who has the coordination and expansion of these efforts as a primary responsibility.

16. What other resources are required to complete this deliverable?

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Consultation	Guidance and project management to develop Cybersecurity standards for K-12	TBD	TBD	State/Federal	grants	
Travel	See exemplar programs in action in other locations.	TBD	TBD	State		
IN CyberPath framework	Cyberseek tool developed for Indiana	TBD	TBD	Grants	Industry donations	

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. The most important benefit of this deliverable would be the coordination of disparate efforts and the contribution that coordinated efforts could make toward keeping the pipeline of talent full.
b. A statewide cybersecurity interactive tool for Indiana
c. Industry-aligned post-secondary student programs at Purdue University's CareerMakers sites.
d. And assessment tool for collecting metrics from industry

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. This would reduce the cybersecurity risk or impact in three ways
   i. Ensuring that all students receive basic exposure to cybersecurity content throughout their time in Indiana schools. We rely on schools to create an educated citizenry. We need our citizenry to have awareness of cybersecurity topics and challenges that is developmentally appropriate.
   ii. Provide aligned exposure to cybersecurity topics throughout the K-12 curriculum including both formal and informal learning opportunities so that more students will consider careers in the area of cybersecurity.
   iii. Provide the opportunity for individuals in the workforce to increase their knowledge in cybersecurity and job opportunities by furthering their education.

19. What is the risk or cost of not completing this deliverable?

a. The risk is having uncoordinated investment in many good things that could have greater effect if considered together. Also, if there is no real attention given to cybersecurity awareness and training at the younger ages of the spectrum, we will have to keep putting out fires and being reactive to real and immediate shortages in the job market.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. A clearly articulated cybersecurity program for K-12 that shows the critical path and skills for cybersecurity and how various opportunities, experiences and curricula can fulfill those critical needs. In addition, optional extensions of core concepts in cybersecurity should also be articulated. Indiana should have a clear map of critical cybersecurity content that clearly shows what topics will be encountered at what ages.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

22. Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

☐No ☒ Yes

a. Indiana would be among the first to implement a cybersecurity curriculum or even to map cybersecurity concepts across the curriculum.

Other Implementation Factors

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. This thinking requires a long view.
b. The actual return on investment is not as direct as some may like.
c. Any results with direct impact to the economy are years away.

24. Does this deliverable require a change from a regulatory/policy standpoint?

☐No ☒ Yes

a. The policy change here would be a formal expectation regarding content and skills about cybersecurity that should be encountered during the K-12 experience.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. An ongoing commitment to revising and amending the cybersecurity curriculum to keep it relevant and responsive to the needs of the workforce and to the needs of society as a whole.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. No formal contacts have been made regarding a coordinated effort on this front although members of the committee are aware of episodic efforts underway.

27. Can this deliverable be used by other sectors?

☐No ☒ Yes

a. If this deliverable is well-executed, other sectors could experience direct and indirect benefit

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. K-12 Schools

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

a. If formal steps were taken in this area, it should be part of the overall effort outlined on the cybersecurity web site.

30. What are other public relations and/or marketing considerations to be noted?

a. Not all families welcome the use of computers in the classroom, and some resist the provision of devices to students. If cybersecurity becomes a curricular emphasis, there will need to be some care given to the education of parents who are concerned that their children are safe and are also concerned about the age-appropriateness of what they know about cybersecurity threats.

Evaluation Methodology

Objective 1: The joint Cybersecurity Task Force ensure more than 75,000 staff and students are delivered training and phishing support through the KnowBe4 platform by December 2024.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: The joint Cybersecurity Task Force will raise awareness of schools to digital threats to the educational process by raising awareness through monthly newsletters, and by working with partners to provide professional development for school IT staff by December 2024.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 3: DOE will work to encourage all schools to appoint one staff member to monitor information releases from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Indiana Information Sharing and Analysis Center (IN-ISAC) by December 2023.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 4: Create a DOE Moodle Community to share school cybersecurity information with public, religious, and private schools as well as provide opportunities for secure collaboration and sharing of best practices by December 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☐ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Update the CHE Cyber Program Data Tool and Report

Deliverable: Update the CHE Cyber Program Data Tool and Report

General Information

1. What is the deliverable?

a. Updated report on the students that are attending Indiana Public, Private, and For-Profit Post-Secondary Institutions in Cybersecurity related fields so that the Indiana Executive Council on Cybersecurity can more fully understand the supply of qualified graduates and their credentials/degrees to make better informed policy decisions.

2. What is the status of this deliverable?

☐ Completed ☒ In-progress 25% ☐ In-progress 50% ☐ In-progress 75% ☐ Not Started

3. Which of the following IECC goals does this deliverable meet?

☐ Establish an effective governing structure and strategic direction.
☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
☐ Strengthen best practices to protect information technology infrastructure.
☐ Build and maintain robust statewide cyber-incident response capabilities.
☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
☒ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. Which of the following categories most closely aligns with this deliverable?

☒ Research – Surveys, Datasets, Whitepapers, etc.
☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. What is the resulting action or modified behavior of this deliverable?

a. Expands the capability of the IECC to fully understand the supply of qualified graduates and their credentials/degrees to make better informed policy decisions.

6. **What metric or measurement will be used to define success?**
    a. If success refers to the deliverable – then timely delivery of report by 3/31/22. Resulting policy decisions.

7. **What year will the deliverable be completed?**
    ☐ 2021 ☒ 2022 ☐ 2023 ☐ 2024 ☐ 2025+

8. **Who or what entities will benefit from the deliverable?**
    a. Most directly the IECC will benefit to make informed policy decisions.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None directly we are aware of. Of note: https://www.nist.gov/itl/applied-cybersecurity/nice

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. None this time but this could change in the future.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Institutions of higher education in Indiana.

12. **Who should be main lead of this deliverable?**
    a. Commission for Higher Education

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of time and resources.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    ☐ One-time deliverable
    ☒ Ongoing/sustained effort

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
CHE team planning meetings, prep and data querying for current program codes	Rajinder Heir, Academic Affairs, Policy & Research	100		Initial inquiries and tasks started in Jul & Aug.
Notification to Academic Officers at Institutions to report Cybersecurity related students/degrees/programs	CHE Academic Affairs		9/30/21	
Begin analysis and synthesis of data from Institutions on Students/Degrees/Programs and develop report on Findings	CHE Policy & Research, Academic Affairs		11/29/21	
Distribute final report	CHE		3/31/22	

Resources and Budget

15. Will staff be required to complete this deliverable?

☐No ☒ Yes

a. CHE staff time required

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
.15		Data Analysis and more			This effort will be to develop the survey, analyze/synthesize the results and provide a report to the IECC. This can likely be accomplished using existing Exempt FTE/Staff. Depending on the ongoing requirements of collecting this data regularly, this is subject to change. Other staff will be involved – coordination, academic affairs team, possibly graphic designer.

16. What other resources are required to complete this deliverable?

Resource	**Justification/Need for Resource**	**Estimated Initial Cost**	**Estimated Continued Cost, if Applicable**	**Primary Source of Funding**	**Alternate Source of Funding**	**Notes**
Office productivity software, graphics software.		No Response				

Benefits and Risks

17. What is the greatest benefit of this deliverable?

a. Regularly reported data on supply of cybersecurity related degree seekers and completers will give the IECC the insight into the supply-side of the equation for Post-Secondary Institutions to understand if policy changes are necessary.

18. How will this deliverable reduce the cybersecurity risk or impact? What are the estimated costs associated with that risk reduction?

a. The state's capacity to insource and grow cybersecurity expertise will mean less financial risk as we will be better able to recruit graduates from Indiana colleges to work for Indiana organizations.

19. What is the risk or cost of not completing this deliverable?

a. If we don't understand the supply-side of the equation, we may have to outsource cybersecurity jobs/contracts to other states and/or countries and/or have to pay higher prices/premiums to accomplish necessary work. If we are unable or unwilling to pay for this work, the State of Indiana and its public and private sectors may be subject to additional risk.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

- Major-level data on cybersecurity-related degrees.
- Minor-level data would also be helpful to understanding the supply.
- Data to understand the extent to which programs have cybersecurity content.

21. Are there comparable jurisdictions (e.g., other states) that have similar projects that we can compare this project to using the same metrics?

☒No ☐ Yes

22. **Are there comparable jurisdictions (e.g., other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?**
☐No ☒ Yes

Other Implementation Factors

23. **List factors that may negatively impact the resources, timeline, or budget of this deliverable?**
    a. If additional deliverables/requirements are placed on staff slated to work on this, it could move the timeline back or risk causing other deliverables to slip in schedule. Having additional resources available would mitigate this, especially for the analysis/report writing part. Potentially, we should have available resources across the entire IECC that can assist in these tasks for various sub-committees and working groups.
    b. We count on the institutions to deliver the data we request in a timely fashion and have no reason to expect this will not happen. However, it is an implementation risk factor.

24. **Does this deliverable require a change from a regulatory/policy standpoint?**
☐No ☒ Yes
    a. We may want to require Institutions to report more granular data than degree-level. This could be codified, but likely will require additional conversations.

25. **What will it take to support this deliverable if it requires ongoing sustainability?**
    a. To support this deliverable in the future, CHE will need to modify its CHEDSS system to account for major-level data and Indiana Post-Secondary Institutions will need to modify their processes to report on these data. It's unclear what the exact effort or financial implications of these changes will be. The CHEDSS system is current under a re-write effort.

26. **Who has the committee/working group contacted regarding implementing this deliverable?**
    a. This deliverable has been discussed internally at CHE at least through the collection of the data. Staff at CHE will now contact Academic Officers at Indiana institutions to collect survey data for the second iteration of the report.

27. **Can this deliverable be used by other sectors?**
☐No ☒ Yes
    a. Less so as it stands, however expanding the collection of this major-level data to non-cybersecurity fields can potentially generate uses for additional domains.

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. Indiana Post-Secondary Institutions should be notified regarding the output of the deliverable.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

☐No ☒ Yes

30. What are other public relations and/or marketing considerations to be noted?

a. None at this time.

Evaluation Methodology

Objective 1: Commission for Higher Education will re-launch survey/tools to capture and collect program course curriculum to help the IECC understand and inventory which higher ed schools are providing cybersecurity related training programs by December 2021.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☒ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Commission for Higher Education will update the Cyber Program Data Tool and Report by March 2022.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group

☒ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☒ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- CHE Cyber Program Data Report 1.0
- Cybersecurity for Education Toolkit 1.0

CHE Cyber Program Data Report 1.0

INDIANA COMMISSION for
HIGHER EDUCATION

Report to the Indiana Executive Council on Cybersecurity

Cybersecurity is at the top of mind for Indiana employers, as well as the state's higher education institutions to ensure the state is producing the necessary talent to meet employer demand and provide a safe and secure digital landscape for all Hoosiers.

While the Indiana Commission for Higher Education had some data on Cybersecurity and related degrees currently being offered in the state, a deeper dive was required to fully understand the options available to students.

Often, Cybersecurity coursework and degree options are "hidden" within other computer and information science programs. With that in mind, the Indiana Executive Council on Cybersecurity's Workforce Development subcommittee pursued a closer look at the richest sources of programmatic data – Indiana's public institutions.

The Commission recently surveyed these institutions to assess how they are prioritizing Cybersecurity content in current and planned computer science and technology curricula. The results of those surveys are summarized in this report.

Several themes emerged in the survey's results about how the state's institutions offer Cybersecurity curricula. Enrollment and graduate numbers, for example, have remained steady or increased over time. And while institutions offer a wide array of education related to technology and computer and information science, a range of Cybersecurity content is embedded in current program offerings.

Enrollment and graduate number highlights

While overall college enrollment has experienced a small decline in recent years (from 65 percent in 2017 to 63 percent in 2019), there has been a steady increase in the number of students enrolling in Information Technology and Cybersecurity-related degrees in Indiana's public and private colleges and universities.

There were over 56,000 enrollments in Information Technology and Cybersecurity-related programs across the state between 2015 and 2019, with Indiana's public colleges representing almost 50,000 of those enrollments. Including the state's private colleges, there were over 7,000 students enrolled in Information Technology and Cybersecurity-related programs between 2015 and 2019 at private, non-profit colleges; and more than 200 were enrolled at private for-profit institutions in the same time period.

Between 2015 and 2019, there were more than 10,600 degrees conferred in the Information Technology and Cybersecurity sectors for all institutions throughout the state. Again, the public institutions provide the majority of those degrees, at just over 9,000. Private, non-profit colleges (1,600 degrees) and private, for-profit colleges (44 degrees) add to the total.

While the majority of conferred degrees in these sectors are represented by Indiana's public colleges, some out of state students come to Indiana specifically seeking these degrees. The state's challenge is retaining those students who come from outside Indiana and encouraging them to stay after graduation.

Indiana's opportunities for going forward and expanding upon these sectors include paying for what we value: including certificates in growing and high-demand areas, such as IT and Business Services, through the state's Workforce Ready Grant.

Additionally, as Central Indiana in particular has become a technology hub in the Midwest, connecting students to local employers who can offer work-based experience and internships will encourage more of these students to make connections and develop roots in the state. This, in turn, provides more opportunity for students to stay in the state after graduation – particularly those that move to Indiana to pursue higher education.

IT and Cybersecurity program enrollment and graduate highlights:

- Purdue West Lafayette anticipates about 150 students graduating with the Computer & Information Technology Degree (with a Cybersecurity major) in 2021 with small numbers of students who switched majors graduating in 2018 and 2019
- Purdue Northwest has 208 students enrolled in the Cybersecurity major as of Fall 2019
- Indiana State University expects to graduate about 20 students from the Cybercriminology and Security Studies program, starting in 2022
- Ball State has a master's of science minor in Computer Security with 25 students enrolled in the spring 2019

Cybersecurity curriculum

A range of Cybersecurity content is included in the current Computer Science curricula for the bachelors of science and bachelors of arts degrees at Indiana's public institutions.

Cybersecurity coursework content ranges from as little as under **6 percent** (Indiana University South Bend) to as much as **over a quarter** of the curriculum (Indiana University Purdue University Indianapolis-Purdue).

The average Computer Science curriculum contains over 12 percent Cybersecurity content and the median Computer Science curriculum contains 10 percent Cybersecurity content.

The state's institutions are also creating new cybersecurity coursework, including a Cybersecurity Minor and Cybercriminology and Security Studies Program at Indiana State University. The University of Southern Indiana created a Cybersecurity Certificate program in the fall of 2019.

By institution: A closer look

The **Purdue Northwest** bachelors of science Computer Information Technology degree program has been recognized by the NSA as a Center of Excellence in Cybersecurity. Purdue Northwest was designated in 2014 and re-designated in 2019 by the U.S. Department of Homeland Security and the National Security Agency as a National Center of Academic Excellence in Cyber Defense Education.

At **Purdue West Lafayette**, the Cybersecurity major has grown significantly between 2016 and 2018. While students began joining the major in the years prior, there were 171 students in 2017 and 232 in 2018. The major represents about 40 percent of the B.S. degree in Computer and Information Technology students in 2018. Purdue West Lafayette has been designated as a Center of Academic Excellence in Research by the U.S. DHS and NSA.

Indiana University and its regional campuses offer cybersecurity courses and degrees ranging from certificates to doctorate-level degree programs. Indiana University has been designated as a Center of Excellence in Cyber Defense and Center of Excellence in Research by DHS and NSA.

At **Ball State University,** the Computer Science degree has a significant focus on cybersecurity, representing 18 percent of the degree coursework. The spring 2019 enrollment in Computer Science was 388 students. The school also offers a master’s Computer Security minor (25 students were enrolled in spring 2019).

Indiana State University’s Information Technology Program has a cybersecurity component which makes up approximately 10 percent of the program’s coursework. The new Cybercriminology and Security Studies Program has grown from 27 students enrolled in fall 2018 to 66 students enrolled in fall 2019.

The **University of Southern Indiana** developed a Cybersecurity certificate program that began in fall 2019. Some classwork in this program is currently a requirement for the Computer Information Science majors.

The **Vincennes University** College of Technology offers a Computer Networking Fundamentals Certificate, which is a one- to two-year certificate with about half of the total credit hours devoted to Cybersecurity content. The university also offers an associate degree for a Computer Network + Security Specialist, with 41% of the total coursework dedicated to cybersecurity.

At **Ivy Tech Community College,** there are options to pursue a certificate, technical certificate and associate degree in Cybersecurity and Information Assurance; the program is focused entirely on cybersecurity. Ivy Tech Community College has been designated by the U.S. DHS and NSA as a Center of Academic Excellent in Information Assurance – 2 Year Education.

Conclusion

As Hoosiers' lives are increasingly connected to digital devices and the Internet of Things continues to gain global traction, the potential threats to Indiana's security also increases. Meeting Indiana's need for high-quality Cybersecurity education and training options must remain a priority for the state's higher education institutions and the state as a whole.

Preparing for the future of Cybersecurity issues in Indiana begins with ensuring there is a sufficient statewide pipeline of talented professionals ready and able to take on the challenge of keeping the Hoosiers safe and secure for years to come.

This is a career path that is in high demand, with more than 2,300 open Cybersecurity positions in Indiana currently, according to the Indiana Cybersecurity Hub. While our public institutions are emphasizing and growing the educational tracks and curricula to support Cybersecurity and related fields, more prominence must be paid to these career paths in order to fill these positions and prepare for anticipated growth in this crucial field.

Cybersecurity for Education Toolkit 1.0

CYBERSECURITY FOR EDUCATION TOOLKIT

Cybersafe Tips & Resources for Indiana's School Communities

Cybersecurity for Education Toolkit

Developed by the Indiana Executive Council on Cybersecurity
August 2020

Table of Contents

HOW TO USE THIS TOOLKIT

Regardless of the important role you play in educating our children and young adults, this *Cybersecurity for Education Toolkit* is designed for you.

Whether you are a superintendent, administrator, teacher, or staff member, we encourage you to use these materials – and share them with your colleagues, students and others in your school community – as a turnkey resource; saving you precious time as you focus on the rapidly increasing challenges that are taking place in education as the school year gets underway.

In fact, we have created the toolkit in a Word Document format that will enable you to cut and paste, copy and/or repurpose all the articles, images, and social media posts in the *Toolkit* as needed.

In addition to these materials, we invite you to visit our Cybersecurity Hub Page located on the website of the State of Indiana at www.in.gov/cyber. There, you will find even more resources – updated frequently -- that will help you with everything from tips on maintaining good cyber hygiene to the steps you should take if you are the victim of a cybercrime.

Developed by the members of the Indiana Executive Council on Cybersecurity (IECC) including the Indiana Department of Education, our Cyber Hub feature sections for Educators (https://www.in.gov/cybersecurity/3827.htm), Teachers (https://www.in.gov/cybersecurity/3836.htm), Students (https://www.in.gov/cybersecurity/3830.htm), and much more!

GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

September 2020

Dear School Community Member:

With the school year underway – inside classrooms and virtually – across Indiana, **cybersecurity** is one of the keys to achieving a higher level of education, safely and securely.

To help our school communities continue to be strong and protected while staying connected, the Indiana Executive Council on Cybersecurity (IECC) along with the Indiana Department of Education has developed this *Cybersecurity for Education Toolkit* for everyone, including:

- Superintendents and School Board Members
- Teachers, staff, and administrators
- Students of all ages and their families
- Every person who lives in our school communities

Our toolkit is designed to be easy-to-understand resource, complete with tips and helpful information to make sure you are cybersafe and practicing good habits that will help:

- Students protect their identity and schoolwork
- Teachers and staff manage their lesson plans and keep safe their student's data, including their grades and assignments
- Administrators protect their students and keep secure their facilities
- Members of the public can engage and communicate with schools and educators

Most importantly, this guide is intended to provide you with resources to get started and more information about online learning. You are also welcome to visit the website for the Indiana Department of Education at https://www.doe.in.gov or check out their *Digital Education Toolkit*. Additionally, there are other materials in the toolkit, including content for use on social media platforms, including Twitter, Facebook, and LinkedIn. Also, we have included a selection of blogs and brief bylined articles – from a variety of trusted sources – that the IECC encourages you to share with teachers, families, and your communities.

You are also welcome to visit Indiana's Cybersecurity Hub Page (www.in.gov/cyber) for an even more resources you'll find valuable -- inside and outside of the classroom. We look forward to your input on this toolkit as we seek to improve it over the coming months and that it will serve as a helpful guide for being safe when you and our children are online.

Sincerely,

Chetrice L. Mosley-Romero
Cybersecurity Program Director
State of Indiana
MosleyCLM@iot.in.gov

Dr. John Keller, CTO, Indiana Department of Education
Workforce Development Committee Co-Chair
Indiana Executive Council on Cybersecurity
jkeller@doe.in.gov

PROTECT YOUR SCHOOL

Article 1:
The Importance of Cybersecurity to Your School's Infrastructure

As a school superintendent, together with your administrators, you are tasked with the day-to-day responsibility of protecting your schools, students, teachers, and staff on behalf of the community.

And, in collaboration with the members of your school corporation's board, you are always working proactively to adopt policies to help ensure that your students learn and are provided with an education in an environment that is safe and secure and that's especially true as it involves **cybersecurity**.

Following on the experiences thrust on schools at the start of the Pandemic, there are a great deal of resources out there to help guide your school's approach to being cyber safe for everything from your infrastructure to the security of your student's personal data, as well as your curriculum and the lesson plans created by your teachers and staff.

According to the National Cyber Security Alliance (www.staysafeonline.info), it is important to routinely evaluate, update, and implement your cybersecurity plans. This includes protecting your schools by following these 10 tips for anyone who relies upon computers in your school district:

- Use anti-virus software.
- Don't open e-mails or attachments from unknown sources. Be suspicious of any email attachments from unknown sources. Also, be suspicious of any email attachments that are unexpected, even if they come from a known source.
- Protect your computer from Internet intruders.
- Regularly download security updates and patches for operating systems and other software.
- Always use hard-to-guess passwords. Mix upper case, lower case, numbers, and other characters not easily found in the dictionary. Make sure your password is at least eight characters long.

- Routinely back up your computer data on disks or CDs regularly.
- Don't share access to your computer with strangers. Learn about file-sharing risks.
- Disconnect from the Internet when not in use.
- Check your security on a regular basis.
- Make sure all your teachers, staff and administrative team members know what to do if a computer or system is believed to be infected or corrupted.

It's also a good idea to raise awareness with your students on why being cybersafe is important and use social media to disseminate information and encourage students, faculty, and staff to learn more about staying safe online visit www.in.gov/cyber, staysafeonline.org, and stopthinkconnect.org.

Article 2:
Collaborate with Your School Board Members About Cybersecurity

For school board members, adopting acceptable/responsible use policies and other important standards related to the use of technology, is at the heart of your responsibilities to the public and the larger school community.

It is important to know that cybersecurity is associated with risks that can catch even the most experienced board members off guard. Cybersecurity treats should be treated like any other kind of risk for your school district. Because of that, the same amount of detail and preparation associated with mitigating financial risks should be implemented when preparing for, conducting, and participating in school board cybersecurity training.

According to *Diligent Insights*, to begin to develop and establish cybersecurity training for your school board, there are core steps that need to be explored and addressed.

Diligent Insights and *K-12 Cyber Secure* highly recommends your school board members collaborate on adopting cybersafe and acceptable use policies for your school community, which include the following:

1. Note any cyber incidents that have occurred in your district the last few years
2. Identify cybersecurity risks and issues that the board and district may face
3. Determine who will be involved in the board's cybersecurity training
4. Develop a plan of action regarding cybersecurity in your school district
5. Identify how to measure the sufficiency and effectiveness of your district's cybersecurity program
6. Determine how much your IT budget is being spent on cybersecurity-related activities and risk management

For more information, visit:

- *Core Steps for Establishing Board Cybersecurity Training* https://insights.diligent.com/cybersecurity-public-education/core-steps-establishing-board-cybersecurity-training.
- *K-12 Cybersecurity: Role of the School Board* https://k12cybersecure.com/blog/k-12-cybersecurity-the-role-of-the-school-board/
- *Campus Safety Magazine* Webinar -- *Here's How an Indiana School District Used Integrated Access Control to Bolster Security* https://www.campussafetymagazine.com/webcast/heres-how-an-indiana-school-district-used-integrated-access-control-to-bolster-security/
- *Indiana Cyber Hub – Education Resources* www.in.gov/cybersecurity/3827.htm

PROTECT YOUR TEACHERS

PLEASE SHARE THE BELOW ARTICLES WITH YOUR TEACHERS VIA NEWSLETTERS, EMAIL, MESSAGE FROM THE SUPERINTENDENT, MESSAGE FROM THE PRINCIPAL, STAFF MEETING, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:
Keeping Your Classroom Secure Online & Using Video

For your dedicated teachers and staff, practicing good cyber hygiene is an important part of the school day and, especially so, when working from home or conducting class remotely.

There are four important steps to keep in mind:

- Beware of Phishing Scams
  - Use caution when opening emails – even those that appear to be from trusted sources or from senders who ask you to provide sensitive information – i.e. share student data or requests
- Encrypt Your Data (both for yourself and your students)
- Secure Your Devices from Physical Attacks
  - Use a VPN (Virtual Private Network) and Multi-Factor Authentication – to provide the greater measure of protection when it is necessary to work from home or out-of-school setting
- Follow Your School's Cybersecurity Protocols
  - Work with your IT staff on system updates/Acceptable Use Policies

Throughout a school district, everyone can benefit from a reminder, to be vigilant when it comes to practicing good habits while working online, including making sure to always:

- **Keep an updated machine.** Having the latest security software, web browser and operating systems is the best defense against viruses, malware, and other online threats
- **Protect ALL devices that connect to the Internet** – It's not just computers, smartphones and other web-enabled devices, it is crucial to provide cybersecurity for your school system's critical infrastructure systems, installed on servers that are separate from those used to store student data and your school corporation's financial systems.
- **Plug and Scan:** Be aware as "USB's" and other external devices can be infected by viruses and malware. Work closely with your IT staff to use your system's security software to scan them (if permissible) or follow your school's policy on removable media.
- **Back It Up:** Protect your valuable work, music, photos, and other digital information by making electronic copies of all information files and storing them safely.

With increasing frequency, as more family members of your teachers and staff work from home, it's important for them to be aware of their surroundings – especially if they are on a video call (i.e. Zoom, Microsoft Teams or WebEx), and that their student's schoolwork is out of view. It is also good to be aware of any potential distractions or conversations occurring in the background.

What's more, teachers and staff are uniquely positioned to educate their students about good cyber hygiene as part of their everyday assignments and in-class interaction.

Be sure the apps and online tools you're recommending your students use meet the basic criteria for safety and privacy before encouraging students and families to download them. It's important, too, to communicate with your students and their families and encourage them to do their due diligence when recommending to them that they download a new educational app, or using an online tool for learning that you've suggested or asked them to use as part of a classroom assignment or homework.

Here are basic tips students can share with their students when safeguarding their online data, including:

ALWAYS HAVE A STRONG PASSWORD

- The first step is to **create complex passwords**. A strong password should be a mixture of upper and lowercase letters and include numbers and symbols, as this will make it less likely to be guessed by cybercriminals. You can use tools like a password meter, which calculate how difficult or easy it would be to guess or hack your password and aim for a high score for each password you create.

- Create **unique passwords for each online account**. For instance, the password for your personal Facebook account should be different from that of your personal email, which in turn should be different from the one you use to access the learning portal at school. This means that if someone guesses or hacks one password, they won't be able to access all of your accounts.

- Try to **change your passwords frequently**. It is recommended to do this at least twice a year, but once every three months is even better and more secure, especially since the sheer number of online accounts accessed at school is so high.

- Creating complex and unique passwords and changing them continuously is a great memory exercise.

- But if it turns out to be too difficult, **try using a password manager** to generate and store your passwords on your device or browser. A password manager uses a special database to create and store strong passwords so you don't have to remember them. But you do have to be careful with that one master password.

- While using public computers or other public devices and networks, **never allow the public computer to remember or store your password**. This can open the door for others to sign in after you and access your online profiles and any other personal information that might have been saved.

- Finally, take advantage of **two-factor verification/authentication** when it is available. These systems typically require you to enter both your password and a special code sent to your phone or email. This type of authentication offers the best protection for those of your accounts that hold personal and sensitive information about you.

DON'T FALL FOR PHISHING SCAMS & HOW TO RECOGNIZE A SCAM

- According to the United States Department of Homeland Security, phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by manipulating them into providing personal information to the attacker.

- There are several ways online phishing scams can happen. Some are through emails, SMS text messages, social media, and even fake tech support phone calls/voicemails.

- The best way to avoid these scams is to not take action based on the email – don't text the number back, don't answer phone calls when you don't recognize the number, and never give your personal information out via email to someone you don't recognize from your contact list. If you keep being targeted by the same number or email, block them, or talk to your cell phone provider about blocking the number from reaching your phone.

But before you can decide not to interact with phishing scams you need to be able to recognize them. Here are a few signs that should make you suspicious:

- **Unfamiliar sources.** If you've never interacted with this person or company before, be wary;
- **Odd email addresses.** Anyone can create a Gmail or Yahoo email account, but an established company will have its own email system: cocacola@yahoo.ph versus name.surname@coca-cola.com;
- **Too many recipients of the same message.** You should be the sole recipient of the email, or at least to know the other few people addressed in case you're not;
- **Direct requests for personal information or money.** Social Security numbers, bank account information or other passwords should not be shared with strangers just because they asked;
- **Text riddled with errors.** Cybercriminals send badly written messages to increase their chances — if grammar and spelling errors don't ring any alarm, someone is more likely to hand over the required personal information;
- **Too good to be true offers.** Murphy's law is not a law for nothing. If something seems unlikely, unrealistic or too good to be true, then it probably is;
- **Strange attachments.** An attachment should be necessary and related to the message. If not, or if the extension is odd (.exe instead of .docx), it's better to not open it.

USE ANTI-VIRUS PROTECTION

- Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems. It includes computer viruses, ransomware, adware, spyware, scareware, worms and more. The damages made by malware vary from making your device more difficult to use by slowing down its functions, to more serious consequences, like controlling your device or stealing your data.

- One rather famous way of malware spreading throughout a school is the use of infected removable drives. As Microsoft's Windows Security noted, "many worms spread by infecting removable drives such as USB flash drives or external hard drives. The malware can be automatically installed when you connect the infected drive to your PC. Some worms can also spread by infecting PCs connected to the same network." Working directly in the cloud is a better option, as long as the cloud is in its turn protected.

- The most important thing you must do is to install antivirus software on all your devices to make sure you're protected no matter what you're using. (Your technology department will likely have done this for you on any device provided by your school.) This will ensure you will avoid many cyberattacks by default or at least you'll get a notification on what seems suspect and needs more attention from your part. As a young adult, it might be hard not to expose many aspects of your personal information online, so protecting your online presence is crucial and worth the costs.

Visit https://www.vpnmentor.com/blog/teachers-guide-to-cybersecurity/ for a "Teacher's Guide to Cybersecurity." For additional resources, you can also visit www.in.gov/cybersecurity/3836.htm.

Article 2:
Working Remotely — How to Be Safe, Secure, and Successful

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

REDUCING RISK ON HOME NETWORKS

Home IT devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

As we continue to work, attend school, and connect with friends and family remotely, there are steps you can take to reduce the risk and improve the security of home networks.

- To help improve the security of your home network, the following is a list of questions to consider. In many instances, you can find answers and solutions online from trusted sources that are FREE and includes step-by-step instructions to help you. You can also consider working with an IT professional as an investment in your cyber safety.

Here’s the list:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models are easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?

- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.
- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?
- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

SECURITY DURING VIRTUAL MEETINGS

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

Sharing of Your Information Assets During Virtual Meetings

- Avoid adding your meeting to any public calendars or posting it on social media
- Require participants to enter an access code
- Avoid reusing access codes or meeting pins
- Distribute the meeting link and access code directly to the intended participants
- Remind invited guests not to share the access code
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information
- Use a privacy shield or cover over your webcam when it is not in use

Managing Your Information Assets and Password Policy

- Use your organization's provided services and devices
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing
- Muting users on entry can prevent potential disruptions
- Prevent users from sharing video by default; allow video sharing only when necessary

- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting
- Do not trust the safety of links shared in meeting chats
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time
- Do not allow attendees to "Join Before Host"
- Set up each meeting to require all attendees to enter a password
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to be sure and protect the connectivity of your devices to protect your personal information!

Taking a proactive approach to following safe cybersecurity practices will help you with addressing key topics, such as understanding the importance of terms, such as "end points" and the prevalence of ransomware attacks – issues and topics that are critical and have become more evident during this new world of COVID-19 with more staff working remotely.

Have you identified more risk than you initially realized? More information and mitigation techniques can be found at Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

PROTECT YOUR FAMILIES

There is no greater responsibility for schools than providing students with a safe and secure learning environment.

At the same time, as part of the new normal, there is never been a greater opportunity to capitalize on the opportunity to educate children and young adults about the importance of digital citizenship and safely communicating online; lessons they can share at home with their families.

At the same time, it's good policy to 1) provide important information digitally to the families of your students – especially for those in elementary school and, *separately*, 2) send out content directly to your middle school and high school students as it relates to classwork, assignments and other relevant school information.

For families, including parents and guardians, it is OK if they are not tech-savvy. If there is something they don't understand, encourage them to reach out to other parents, to their child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

For more information about how you can assess your cybersecurity knowledge as an individual or an organization, visit www.in.gov/cybersecurity/3826.htm.

SHARE THE FOLLOWING ARTICLES WITH STUDENT PARENTS & GUARDIANS INCLUDING YOUR LOCAL PARENT SUPPORT GROUP OR PARENT TEACHER ASSOCIATIONS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:
Keeping Your Child Cyber Safe at Home

With so many changes in the last several months, it has become even more important for families to make their homes more secure when connecting online for school and work.

As families, including parents and guardians, try to navigate these more virtual times, it is OK if they are not tech-savvy. If there is something you don't understand, reach out to other parents, to your child's school, or trusted family members. The goal here is not to make them or the student a security expert, but to make online learning a safe space.

The National Cybersecurity Alliance offers eight tips to share with families, including:

- NEW TECH? If the school issues or requires a technology that you and/or your child are not familiar with, explore its features together. Configure the security and privacy settings together immediately.

- APPLY YOUR RESEARCH. Apps are a great way for students to learn and apply their knowledge. Before downloading any new learning app on your child's device, make sure it is a legitimate app. Who created the app? What do the user reviews say? Are there any articles published online about the app's privacy & security features (or lack thereof)?

- DON'T HESITATE TO UPDATE. Having the latest security software, web browser, and operating system on devices children are using for their virtual schooling is one of the best defenses against online threats. When the computer or device says it's time to update the software, don't click postpone. Update.

- STRONG PASSWORDS IN PLAY KEEP CYBER CRIMINALS AT BAY. When is the last time you changed your home's router password, if ever? Change passwords for routers and smart devices from their default manufacturer's password to one that is long (at least 12 characters) and unique.

- PARENTAL CONTROLS. Parental controls are a great way to establish parameters around what kids can and can't do online. They do not replace candid discussions with your kids about online security and safety. Children may not recognize the dangers of visiting unknown websites or communicating with strangers online, so talk with them about these threats.

- NETWORK SEPARATELY. Students are not the only ones spending more time on the home network. Parents are also working from home at an unprecedented scale. *If you and your children are all working from home, consider using separate networks to enhance your security--particularly if your work involves access to sensitive information.*

- KNOW YOUR ROLE. Sometimes it is unavoidable for children to use the same computer that parents use for their work. If you are sharing devices, set up different user accounts so that children have access to a guest account with limited permissions and access. For instance, restrict your child's ability to install and run software applications.

- CONFIGURE PRIVACY SETTINGS. Go through accounts with children to configure privacy and security settings to limit over-sharing of information--such as location and camera sharing. Walk the kids through why certain settings need to be changed.

For additional resources, visit www.in.gov/cybersecurity/3832.htm.

Article 2:
Keep Your Elementary Student Cyber Safe

Elementary students have grown up surrounded by electronics and the internet. From games and videos on a tablet to synchronous Zoom calls with their third-grade class; young students are subjected to cyber risks everywhere.

Incorporating good cyber habits at a young age, particularly as the workforce becomes more embedded in the internet, will prevent hacks, theft, and fraud in the future.

Parents are the guiding force when it comes to teaching kids how to be safe when they are online. Introducing good cyber habits can be as simple as playing fishing games to teach about the dangers of "phishing" scams. Here are a few examples of how to teach cybersecurity tips to children, and how parents can protect children:

- Understanding passwords: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- The App Store: There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

While children may not seem like a main target of bad actors, they can be vulnerable. Child activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

Article 3: Keep Your Middle School and High School Student Cyber Safe

Just as they did while in elementary school, students, today, are familiar – and somewhat tech-savvy – when it comes to computers and being online, both for schoolwork and socially.

And, as students become teenagers, they are more likely to go places without their parents or even an adult. The same is true with the amount of time middle and high school students spend on their laptops, tablets, and phones.

Working with your child is key, especially as it involves being aware and having conversations with them about the sites they are visiting and who they are communicating with.

Tips include:

- **Understanding passwords**: It can become a habit, especially in children, to create one "master password" for all devices and accounts to make them easy to remember. And while passwords are often controlled and created by parents rather than children, it is important to ingrain the concept of having unique and *complicated* passwords for all accounts and devices to protect information.

- **Protecting personal information on social media**: It can be tempting to make funny posts on TikTok that reference the names of friends, names of schools, etc., but this can be incredibly dangerous. Social media is the newest form of communication for kids and adults alike, but it's also an easy way for people to gather information that can be used by bad actors for a variety of things. It's important to teach kids that personal information is *personal* and shouldn't be shared online.

- **The App Store:** There are thousands of apps and games that can be accessed through tablets, computers, and cell phones. However, not all of these are meant for children. Be sure that content restrictions are set in place through online accounts to ensure that only kid-friendly content is in the hands of kids.

While children and teens may not seem like a main target of bad actors, they can be vulnerable. Adolescent activity on unprotected networks can be a gateway for the bad guys to sensitive information such as financial records or other data. It is important to introduce these concepts early so that both you and your children can remain safe.

Article 4:
Nine Ways to Cope with Working from Home with Kids

Even before the Pandemic began, it was not unusual for family members, working from home, to be sharing space with their children, who, upon arriving home from school, are starting on their homework and class assignments.

Within the past six months, the number of people working remotely increased dramatically and it is expected to likely grow as the impact of the Pandemic continues to impact everyone across Indiana and around the world.

To help working parents adjust to the "new normal" a recent MSNBC article highlighted 9 tips for parents working at home with children (https://www.cnbc.com/2020/03/17/working-at-home-with-kids-during-covid-19-crisis-with-kids-underfoot.html). Among the suggestions involving shared workspace, it is suggested:

1. **Be upfront about expectations**. It's important to proactively communicate with your employer that your children are at home so they are aware that you cannot guarantee your work or work calls will be interruption-free. This applies to children as well: Explain to them that working from home means you really are trying to do work. While it may seem like a regular weekend or a vacation day because you are all at home, these are highly unusual circumstances.

2. **Set up virtual babysitters.** Reach out to friends, aunts, uncles, grandparents, babysitters, teachers. These individuals are amazing resources, because you can use them to arrange virtual playdates for your kids. They can talk, read, play games, sing, do dances and much more, all online.

3. **Plan activities that don't need supervision.** Different activities apply to different age groups, of course, depending on your schedule and the age of your children. While babies will give you a breather during nap times, you can rely on swings and bouncy chairs or put on music or Baby Einstein. Create activity boxes that contain games and puzzles that require minimal adult supervision for toddlers and grade-schoolers. Older kids will most likely be busy with online schooling.

4. **Prioritize your schedule.** Aim to schedule your most engaging/reliable activities for the kids to be on their own during the time you need to be most productive.

5. **Split the work.** If you have a partner, and if your work allows, you may consider taking shifts. For instance, one person watches the kids in the morning while the other works, and vice versa in the afternoon. This can better guarantee at least some hours where your focus is purely on work.

6. Reward good behavior. Working from home with kids means maintaining harmony however possible, and this includes setting up a reward system for them when they follow directions.

7. Take mini breaks. Consider temporarily changing your style of working. Instead of tackling a project for three hours, break up the day more to give your children the attention they need. Honor the fact that their attention spans are short, so your work will likely need to be done in chunks. Expect that you may need to continue working after they've gone to bed or wake up earlier in the morning to get more uninterrupted hours in.

8. Stress less about screen time: Under normal conditions, many parents limit screen time. It is worth considering adding to their daily screen time allotment to buy you more work time. Just explain to your children, though, that it is a temporary adjustment.

9. Get creative with office space. Try to find a space with a door that can be closed. Creating physical boundaries can help reinforce the message that you need to be working. Anyplace in the house with internet access can act as an office during an emergency, especially for when you have to ensure calls are uninterrupted.

Article 5: The New Normal — Sharing Your Workspace with Your Kids

Growing up, it was bit of a big deal if you had an opportunity to go to the "office" with your Mom or Dad. The experience might have had a bit of a mystique to it.

Fast forward to earlier this spring, as the Pandemic began to take hold, the mystery was solved, as many companies sent their employees home to work remotely. And, at the same time, schools shifted from in-person, classroom instruction to e-learning at home.

Now, as a lot of families prepare to continue sharing space, working from home while your kids do their homework *is* the new normal. That said, there are a few things to keep in mind as you prepare for what, more and more, could become a way of life for some time to come.

When it comes to setting up an office, one of the first things that usually your company takes care of is the cybersecurity. But, when you work from home, you'll want to pay close attention to a few important tips, including:

- Always practicing good cyber hygiene by using antivirus software
    - Unfortunately, cyber threats are not on a pause. In fact, there is a clear spike in phishing and other cybercrime activity now that most people are working from home.
    - Make sure your systems and programs are up to date
- Ensure your home network is encrypted
    - Make sure, too, your router is protected with a secure password and if your router is more than 2 years old, you will want to replace it to provide the best protection
- Ensure your privacy with a Virtual Private Network (VPN) preferably issued by the company) to make sure your connection is protected along with your data and ALWAYS use it when connecting to a public Wi-Fi network
- Avoid oversharing your screen, especially during any online meetings and be sure that you haven't left any windows open with content that you wouldn't otherwise share. The same protection is there for any company information that might be proprietary
    - Be sure to maintain the same privacy, as it regards your children's schoolwork, along with any discussions you have online with their teachers and that it does not conflict with your work (i.e. online meetings)
- Beware of COVID-19 related scams, as It has been the topic of numerous international and national phishing and scam campaigns. If you get emails with any suspicious links or attachments related to Covid-19, don't open them

- Be sure not to share any personal information in messages, emails or on social media and make certain that the person requesting any information really did so before sending out what is known as PII – personal identifying information
  - It is also a risk to share pictures of your remote working station in social media. You might accidentally share important information while you do it.
  - Same is true with using your webcam. With webcams, you might also accidentally share too much about your home or your family members.
- Create a safe, comfortable environment for your kids – and yourself
  - As part of the approach, consider allowing your kids additional screen time, with the understanding that it is not a permanent situation, but they'll appreciate experiencing some added flexibility
- Working from home requires changing your routine and make sure your cybersecurity is part of that.

For additional resources, visit www.in.gov/cybersecurity/3832.htm.

Article 6:
Working Remotely – How to Be Safe, Secure, And Successful

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

REDUCING RISK ON HOME NETWORKS

Home IT devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

As we continue to work, attend school, and connect with friends and family remotely, there are steps you can take to reduce the risk and improve the security of home networks. Consider the following list to gauge the amount of risk involved and improve the security of your home network:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models are easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?
- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device’s administration page?
- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.
- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn’t provide any identifying information?

- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

SECURITY DURING VIRTUAL MEETINGS

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience.

Sharing of Your Information Assets During Virtual Meetings

- Avoid adding your meeting to any public calendars or posting it on social media
- Require participants to enter an access code
- Avoid reusing access codes or meeting pins
- Distribute the meeting link and access code directly to the intended participants
- Remind invited guests not to share the access code
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information
- Use a privacy shield or cover over your webcam when it is not in use

Managing Your Information Assets and Password Policy

- Use your organization's provided services and devices
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing
- Muting users on entry can prevent potential disruptions
- Prevent users from sharing video by default; allow video sharing only when necessary
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting
- Do not trust the safety of links shared in meeting chats
- Schedule "Unlisted" meetings and hide specific details, such as its host, topic, and starting time
- Do not allow attendees to "Join Before Host"
- Set up each meeting to require all attendees to enter a password
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting

- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to lock down connectivity devices to protect information assets! A resilient cybersecurity mindset contributes towards being able to have a clear view of the objectives. For some, end points might have become a primary concern, for others, the corporate assets might have become even more susceptible in light of the increased amounts of ransomware. This dual pronged problem especially became more evident during this new world of COVID-19 with more staff working remotely.

Have you identified more risk than you initially realized? More information and mitigation techniques can be found at Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

PROTECT YOUR STUDENTS

SHARE THE FOLLOWING ARTICLES WITH STUDENTS VIA EMAIL, NEWSLETTERS, ANNOUNCMENTS, ETC. THROUGHOUT THE SCHOOL YEAR.

Article 1:
Protecting Yourself Online

Whether you are a sixth grader entering middle school or a senior preparing for graduation, you have grown up surrounded by electronics of every variety and the Internet.

From games and videos on a tablet to completing your homework and engaging others on social media, you are online, often for hours at a time each day. And, while it's OK to have fun, whether you're on your laptop or phone, at school or at home, there are several things you can do to protect yourself from people who are looking to steal your identity or target you for abduction or worse.

Here are some helpful tips from Norton (a recognized authority on cybersecurity):

- Don't use the same password twice
- Direct messages from unknown accounts are usually not reliable. Report and block these accounts and be sure to *not* open any links they send.
- Avoid sharing too much personal information like where you live, your whole name, what time you are home alone, etc.
- Put a lock on your phone – a pattern, a code, facial recognition etc.; this will ensure that, if your phone is taken by another person, they cannot access your phone, personal data or your social media accounts.
- The block button is not something to fear! It will help keep bad people away from your information, keep you safe, and your feed uncluttered

For more, visit www.in.gov/cyber.

Article 2:
Don't Get Hacked

When you're at school or you are working on completing your class assignments, there are some important things you can do to make sure your computer is protected against viruses and hackers and you are not exposed to any sort of security risks (like someone hacking your microphone or camera to take illegal audio and video of you).

- Enable Automatic Updates so your computer is the most secure
- Shut down or restart your computer once a week to allow updates to take effect
- For all your devices, remember to backup your photos, documents, etc. in case you lose your device, or it gets hacked and you have to erase your device.
- Always install updates when your carrier tells you they are available
- Be sure to always use legal filesharing services for obtaining music, movies, TV, games, books, etc. on the Internet. A large list of digital music, videos, and other services is available from Educause at http://www.educause.edu/legalcontent. If you use illegal services, know that many people include links to malware to hack your computer.
- When you are not using your computer, turn it off. If you are using your computer, put a protective cover on your webcam so it *cannot* take pictures of videos without you knowing.

For more helpful tips for protecting yourself online, be sure to check out https://its.ucsc.edu/security/student.html. You can also learn to best protect yourself on social media, by looking over a *Social Media Guide* and additional resources at https://www.in.gov/cybersecurity/3830.htm.

Article 3:
Top 5 Cyber Tips for To Start NOW

Whether doing research, finishing assignments, emailing teachers or classmates, or just communicating, your computer and phone is a gateway to a lot of problems you don't need, especially now.

Here are five cybersecurity tips for students according to MYKI.com (a reputable digital identity management company):

1- Be careful what you share

You might want to consider the impact of what you post online. We'd all like to show off that we passed our driving test, or that we're going on vacation, but posting pictures of things like driver's licenses, boarding passes, or credit cards makes you a prime target for identity theft.

2- Lock up and shut down

Leaving your laptop or phone unlocked is a big mistake. The damage might be as minor as your annoying roommate changing your Facebook profile picture to something silly, or as major as some stranger in the cafe you're working at messing with your bank account. If you're going to leave your laptop or phone unattended, make sure you lock it, or set it to sleep or shut down after a certain period of inactivity.

3- Avoid phishing emails

Think twice before you reply to that Nigerian prince.

There are plenty of thieves and scammers on the web, and phishing emails are one of their tried-and-true tactics. These are emails that might look like they're from a trustworthy source, but are actually trying to trick you into providing sensitive data, like your password or credit card details.

All you have to do to prevent yourself from being "phished" is have some common sense and make sure the sender of an email is really who they say they are.

4- Stick to HTTPS websites

Here's something you may have never stopped to consider. Look up at the address bar of your browser: the URL begins with "https".

This means that unlike HHTP protocol websites, the site you're currently on uses a secure protocol, and all communication between your browser and that site is encrypted. In other words, no third party can eavesdrop on you and intercept the data you provide that site. That's not to say that all HTTP websites are malicious, but it's always best to proceed with caution.

5- Use a password manager

Last but not least, you'll need to get yourself a good password manager.

On top of the dozen social media accounts you've already got, you're probably going to need some new academic accounts, which means a *whole lot* of passwords to remember.

But since you're only human, you'll be very tempted to use the same easy-to-remember password for everything, which is actually quite risky.

This is why it is highly recommended that you use strong and unique passwords, which you can securely store with a password manager.

For more information, visit www.in.gov/cyber.

SOCIAL MEDIA CONTENT #4YOU2SHARE

Social media is a platform for learning, especially when it comes to cybersecurity.

And, whether you're sending out a Tweet, sharing a post on Facebook, or you have information to provide to others in the business world on sites, such as LinkedIn, it's important that you make sure you are communicating in a way that is safe and secure.

Although it is true that good advice can often be shared in as little as 40 characters or to a link that takes you to a credible source, so, too, it's important to follow best practices whenever you are online.

Here is some content and quick links we invite you to share with your family, friends, colleagues, and community members. You can use this content on your social media platforms or as part of any digital newsletters and other communication you are providing to families and students.

Content for Students

- Read the *Social Media Guide for Students, Parents, and Bloggers* at https://www.cisa.gov/sites/default/files/publications/Social%20Media%20Guide_1.pdf

- Cyberbullying is not a thing of the past. Learn how young people can identify and protect themselves from cyberbullies here: https://www.us-cert.gov/ncas/tips/ST06-005 #cybersecurity #stopcyberbullying

- Cybersecurity Tips for Teens & Families: Things I Wish My Parents Had Told Me About Internet Safety. https://www.netliteracy.org/safe-connects/collateral-material/?gclid=EAIaIQobChMImZuxmZqR6wIVjsDACh3XIARIEAAYAiAAEgIBlPD_BwE

- Back to school season is coming right up! Pens and pencils are important, but so is staying cyber safe! Learn more student cyber safety here: https://securityboulevard.com/2019/08/back-to-school-tips-the-abcs-of-online-security/ #cybersecurity #backtoschool

- Series on Student safety
  - https://ets.hawaii.gov/wp-content/uploads/2016/09/Cyber-Tips-for-Students.pdf
  - https://www.us-cert.gov/ncas/tips/ST06-005
  - https://www.marquette.edu/remote-learning/cyber-security-tips.php. - remote learning

- Cybersecurity Tips for Student Bloggers https://staysafeonline.org/blog/cybersecurity-tips-student-bloggers/

Content for Parents

- 5 Cyber Safety Tips Every Parent Should Know.

- Top 5 Questions Parents Have About Cybersecurity https://www.connectsafely.org/wp-content/uploads/securityguide.pdf

- Tips for Parents - Protecting Kids Online https://www.consumer.ftc.gov/topics/protecting-kids-online

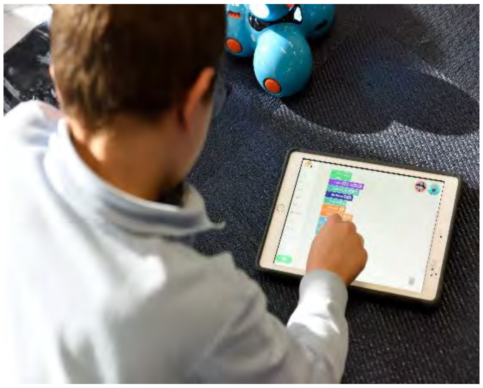
- 13 Apps Every Parent Should Know in 2020 https://educateempowerkids.org/13-apps-every-parent-should-know-in-2020 #cybersecurity

- Parents: With kids spending more time online, it is important to teach them how to be cyber safe. Learn more about social media safety here https://au.norton.com/internetsecurity-kids-safety-parents-best-practices-to-social-media-security.html #cybersafe #cybersecurity #cyberaware

- Tips for Parents Raising Privacy-Savvy Kids https://documentcloud.adobe.com/link/review?uri=urn:aaid:scds:US:09e0015f-3bc7-4504-b008-88692c8ef737

Images for Social Media

As you use the social media content and develop your own content for your school district with the many tips in the *Cybersecurity for Education Toolkit*, feel free to copy and paste the below images with your messages.



SCHOOL COMMUNITY PATRONS

Who are your school community's patrons? They are the people who help make up your town or city; everyone from your grandparents to that young couple who just moved in next door.

In other words, it is everyone who is *not* a student, teacher, staff member, administrator, or school board member. Yet, they are invested in living in a place that values education and understands that good schools contribute to the quality of life within the community.

School districts routinely communicate information with people through newsletters, stories in the news media and through their family members and friends.

Because of this, it is important for members of the public to know and understand the importance of being cybersafe and there are resources out there for everyone.

STOP. THINK. CONNECT. ™ is the global online safety awareness campaign to help all digital citizens stay safer and more secure online. The message was created by an unprecedented coalition of private companies, non-profits and government organizations with leadership provided by the National Cyber Security Alliance (NCSA) and the APWG.

The campaign was launched in October of 2010 by the STOP. THINK. CONNECT. Messaging Convention in partnership with the U.S. government, including the White House. NCSA, in partnership with the APWG, continue to lead the campaign. The Department of Homeland Security leads the federal engagement in the campaign at:
https://stopthinkconnect.org/

For additional resources, visit www.in.gov/cyber.