INCIDENT RESPONSE IS A TEAM SPORT EVENT SCHEDULE
NEW COLLEGE INSTITUTE
191 FAYETTE STREET, MARTINSVILLE, VA 24112

MARCH 30, 2023

Baldwin Hall

9:00 – 9:30 – Light Breakfast, coffee

Opening Remarks: NCI Speaker & VSTE and VDOE

9:30 to 12:00 – Martin-Lacey Lecture Hall
Strengthening Your Incident Response Plan through Tabletop Exercises

Dr. Tara Nattrass (Dell Technologies) & Dr. David Raymond (Virginia Tech Cyber Range)
When faced with a cybersecurity attack, leaders need to be prepared to respond and recover. During this session, we will engage in a facilitated, discussion-based cybersecurity tabletop exercise. This exercise will lead to an opportunity to draft and/or review and update your Incident Response Plan (IRP) with feedback from colleagues from other divisions as well as agency and organization cybersecurity experts. We will further develop division Incident Response Plans while strengthening connections among agencies, organizations, and school divisions.

LUNCH: 12- 1 pm

BREAKOUTS:

1:15 PM to 2:45 PM – Room 1
Operational, Legal, and Communication Issues – (for school administrative leaders)
Phillip Harmon, Associate, Woods Rogers Vandeventer Black PLC, Roanoke, VA

Participants: Superintendents, Directors of Instruction, School leaders…

Cybersecurity incidents vary in size and scope but have catastrophic potential to derail School System activities.

> While IT and computer professionals fight through technical remediation and forensic efforts, school leadership often faces pressing and difficult operational decisions. How are the leaders of your District prepared to respond to an incident? This presentation will examine the different roles and considerations various members of School District leadership might encounter when faced with a large cybersecurity attack. Topics range from the attorney-client privilege, legal notification obligations, cybersecurity budgeting, crisis communications, how to

handle instructional impacts, and more. Preparation before a major cybersecurity event can help improve familiarity and the quality of decision-making when stakes are high. Superintendents, assistant superintendents, CAOs, Finance, and HR professionals are all invited to join (and bring questions to) this critically important conversation.

1:15 PM to 2:45 PM, Room 2
Technical Simulation – (for School Technology Leaders)
Sergio Orellana, BinaryLab

Participants: CTO's, CIO's, technology directors, network administrators, other technical staff

Historically, tabletop exercises focus on policy availability and creation in response to cyber events.

At BinaryLab, we use interactive, real-world simulation software to generate user and network traffic to mimic what an external, unauthorized user may do in a network. In this exercise, participants and their network defense tools will be confronted with a scenario where it will be difficult to distinguish between an authorized human-user interaction vs that of a computer or automated response within an environment. The latter is meant to mimic potential reconnaissance, lateral movement, and creation of backdoors akin to precursors of a ransomware attack. To that end, at BinaryLab, we aim to create exercise traffic patterns that would realistically mimic typical human behavior. Those activity patterns would be random enough to challenge administrators and network defenders to properly discern whether humans and the deployed security technology detect and identify the legitimacy of the activity generated. Furthermore, we aim for a level of realism that allows participants to sufficiently determine and associate the intent of network actions with a particular user. The goal is to construct complex scenarios where different people can play different roles within an exercise like a traditional tabletop exercise. This will enable the audience to think of their network environments and the technical and administrative safeguards they have in place to deter this type of activity.

3 to 3:30 End of Day /Closing
Presenters :

Take aways, questions, action steps –

- What to do upon return to school divisions?
- Allocating funding for cybersecurity
- Refine IRP after everyone has a shared experience.
- Tabletop with reflection to help people walk away with something concrete.
- What outcomes do you want to see from your IRP?