# COMMUNITIES AT RISK FOR CYBER ATTACK: **HOW LOCAL ELECTED OFFICIALS CAN BUILD CYBER RESILIENCY**

**WEBINAR**
**AUGUST 11, 2020**

PRESENTED BY THE MARK O. HATFIELD NSA/DHS NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBER RESEARCH

## MODERATOR

**MARGARET E. BANYAN**
**Ph.D, Senior Fellow**
Center for Public Service, PSU

## PANELISTS

**BILL BAERTLEIN**
**Tillamook County Commissioner**

**RONALD BUCHANAN**
**Chief Information Security Officer,**
St. Charles Health System

**BARBARA ENDICOTT-POPOVSKY**
**Ph.D., Sr. Principal Research Scientist,**
Cybersecurity

**RALPH JOHNSON**
**CISSP, HISP, CISM, CIPP/US**

VIEW RECORDING

**Please offer your feedback through this quick survey (1 minute)**

## KEY POINTS

**CYBER ATTACKS**

- Cyber-readiness of the nation is dependent on the cyber-readiness of local governments; attacks infiltrate at the local level, instead of targeting the national level.
- A cyber attack can happen to anyone and may even already be happening without your knowledge.
- Tillamook County Response: Recognized the attack, activated Incident Command Team, assessed the extent of the breach, established one person to liaise with the press, contacted insurance company and support agencies, determined the extent of the damage before negotiations, evaluated cost to restore lost data internally vs paying the ransom, ruled out whether the breach was caused by a terrorist organization, sent encrypted file to prove it could be restored, negotiated details of transfer (Bitcoin), and received and restored files.

**STRATEGIC PLANNING AND PROCEDURES**

- Assess security v. risk in order to prioritize resources. Instead of looking at it as a compliance problem, look at it as a risk problem. Do a risk assessment (internal or by a third party), identify which are the most vulnerable/ important parts of your jurisdiction and prioritize those. Health records? Infrastructure such as power, water, internet? Prioritize what makes sense for your community.
- Take a proactive approach: run table top exercises, prepare for business continuity. Identify which operations are essential and how to continue them for two weeks - a month without computers, internet, or phones. Have a checklist worked out in advance of all the things you need to do when you realize there has been an attack.
- Confirm your backups are secure and that they go offline when they are done.
- Contact your insurance company and ask which measures, policies, procedures you need to have in place and what your policy will cover.
- From a policy standpoint: build a cyber-readiness framework into your strategic planning and budgeting process; if you don't, the topic never makes it to your elected officials.
- Consider cloud-based services, especially for smaller jurisdictions.

**SAVE THE DATE**
NOVEMBER 10TH, 2020

# COMMUNITIES AT RISK FOR CYBER ATTACK: **HOW LOCAL ELECTED OFFICIALS CAN BUILD CYBER RESILIENCY**

**WEBINAR**
**AUGUST 11, 2020**

PRESENTED BY THE MARK O. HATFIELD NSA/DHS NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBER RESEARCH

## MODERATOR

**MARGARET E. BANYAN**
**Ph.D, Senior Fellow**
Center for Public Service, PSU

## PANELISTS

**BILL BAERTLEIN**
**Tillamook County Commissioner**

**RONALD BUCHANAN**
**Chief Information Security Officer,**
St. Charles Health System

**BARBARA ENDICOTT-POPOVSKY**
**Ph.D., Sr. Principal Research Scientist,**
Cybersecurity

**RALPH JOHNSON**
**CISSP, HISP, CISM, CIPP/US**

**VIEW RECORDING**

**Please offer your feedback through this quick survey (1 minute)**

## KEY POINTS (CONT.)

**STAFF READINESS**

- Cybersecurity awareness program for all employees (not just IT). The greatest vulnerabilities rely on the culture: human element (employees handing login credentials over to cyber criminals). Culture eats policy for breakfast: build a risk focus into your culture.
- It's essential to have at least one tech-savvy staff member who is able to manage a contract for outsourced services, to confirm that you're contracting for the right things, and that you're getting them!

**CAPACITY BUILDING**

- If you don't know where to start, find a mentor (from the state, trusted partners, outside the state); they can advise where to start based on your agency's level of maturity.
- Consider working with your local universities and community colleges to identify resources and collaborate.

**LIST OF RESOURCES:**

- Multi-State Information Sharing & Analysis Center
- Oregon Cyber Security Services - OSCIO
- SANS
- Center for Internet Security
- Information Systems Security Association International
- ISACA
- Essentials of Cybersecurity
- National Initiative for Cybersecurity Education (NICE)
- FBI INFRAGARD
- Cybersecurity & Infrastructure Security Agency (CISA)
- National Cybersecurity Alliance Stay Safe Online
- Mark O. Hatfield Center for Cybersecurity NSA/DHS National Center of Academic Excellence in Cyber Research
- PSU Center for Public Service Fellowship Programs

**SAVE THE DATE**
NOVEMBER 10TH, 2020

Portland State
Hatfield School of Government