COUNTY OF HUMBOLDT

For the meeting of: 5/19/2020

File #: 20-534

To: Board of Supervisors

From: Human Resources

Agenda Section: Consent

SUBJECT:
Authorize Annual Mandatory Cyber Awareness Training Requirement

RECOMMENDATION(S):
That the Board of Supervisors:

1. Authorize Human Resources, in collaboration with the County Information Technology (IT), to require all county employees to complete 1-hour of Cyber Awareness Training annually effective immediately.

SOURCE OF FUNDING:
N/A

DISCUSSION:
Employee Cyber Awareness Training greatly enhances IT Security posture, standing in the way of cyber criminals. In 2017, the FBI's Internet Crime Complaint Center (IC3) received 1,783 ransomware complaints that cost victims over $2.3 million. Those complaints, however, represent only the attacks reported to IC3. The actual number of ransomware attacks and costs are much higher. In fact, there were an estimated $184 million ransomware attacks last year alone. 91% of successful data breaches started with a spear phishing attack. Ransomware damage costs are predicted to reach $20 billion by 2021.

Voluntary training only solves part of the problem. Over the past nine months, 48% of County Employees (with the exception of DHHS and DCSS) have completed voluntary cyber awareness training. A county-wide annual training mandate will ensure that all county users understand how to identify malicious e-mail and other IT Security concerns. There are significant and ever-increasing liabilities associates with cyber security and training employees is one of the most important measures that the County of Humboldt can actively participate in.

County employees are mandated to complete annual security awareness training per the following regulations:

Code of Federal Regulations Title 45 Chapter A Subchapter C Part 164 Subpart C Section 164.308 Administrative Safeguards § (a)(5).

I. Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
II. Implementation specifications. Implement:
    a. Security Reminders (Addressable). Periodic security updates.
    b. Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.
    c. Log-in monitoring (Addressable). Procedures for creating, changing, and safeguarding passwords.

Department of Health Care Services (DHCS) Medi-Cal Privacy and Security Agreement ACL 19 -16 § (II)(A) Employee Training.

Train and use reasonable measures to ensure compliance with the requirements of this Agreement by County Workers including, but not limited to:

1. Provide initial privacy and security awareness training to each new County Worker within 30 days of employment
2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all County Workers. Three or more security reminders per year are recommended;
3. Maintain records indicating each County Worker's name and the date on which the privacy and security awareness training was completed and;
4. Retain training records for a period of three years after completion of the training

Internal Revenue Services (IRS) publication 1075 § 9.3.2.2 Security Awareness Training.

The agency must:

1. Provide basic security awareness training to information systems users (including managers, senior executives, and contractors):
    a. As part of initial training for new users
    b. When required by information system changes
    c. At least annually thereafter
2. Include security awareness training on recognizing and reporting potential indicators of insider threat

California Department of Public Health (CDPH) Information Security Policies § 300 Awareness & Training.

In addition to CDPH Policy, Information privacy and security training is required for all employees by both State and Federal laws and regulations. This includes, but is not limited to:

1. State Administrative Manual (SAM) Section 5300.3, Agency Responsibilities, #6, "Maintain a security and ongoing privacy program including an annual training component for all employees and contractors. Refer to Government Code 11019.9 and Civil Code 1798 et seq."
2. SAM Section 5325, Human Resources Security, "Each agency is responsible to provide security roles and responsibilities to employees, contractors and third party users. This will ensure the users are informed of their roles and responsibilities for using agency information assets, to

reduce the risk of inappropriate use, and a documented process to remove access when changes occur. Personnel practices related to security management must include: #2 Training of agency employees, contractors, and third parties with respect to individual, agency, and statewide security responsibilities and policies."

3. HIPAA Security Rule, 164.308(a)(5)(i), "security training will be required for all staff, including management. Training would include awareness training for all personnel, periodic security reminders, user education concerning virus protection, user education in the importance of monitoring login success/failure, and how to report discrepancies and user education in password management.

Upon your Board's approval, Human Resource will work with the Information Technology Division to ensure that up to date training content is made available to meet these mandates.

FINANCIAL IMPACT:
There is no financial impact other than staff time taken to complete the training.

STRATEGIC FRAMEWORK:
This action supports your Board's Strategic Framework by providing for and maintaining infrastructure and investing in county employees.

OTHER AGENCY INVOLVEMENT:
N/A

ALTERNATIVES TO STAFF RECOMMENDATIONS:
Your Board could choose to not authorize the requirement of annual mandatory Cyber Awareness training for all county staff. This is not recommended as a great deal of liability exists that can be mitigated with staff training.

ATTACHMENTS:
None

PREVIOUS ACTION/REFERRAL:
Board Order No.: N/A
Meeting of: N/A
File No.: N/A