CalHFA's 2021 Cybersecurity Update

Russell Nakao
Chief Information Security Officer
rnakao@calhfa.ca.gov

Ashish Kumar
Chief Information Officer
akumar@calhfa.ca.gov

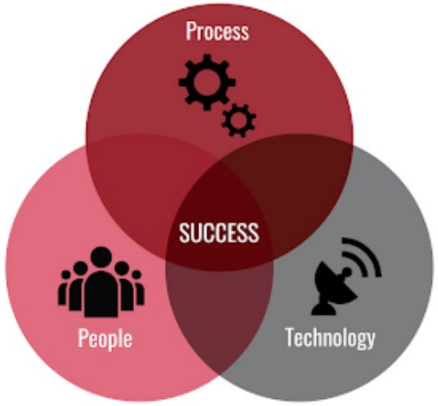
Agenda

- Cybersecurity
- Mitigating Cybersecurity Risk at CalHFA

Cybersecurity

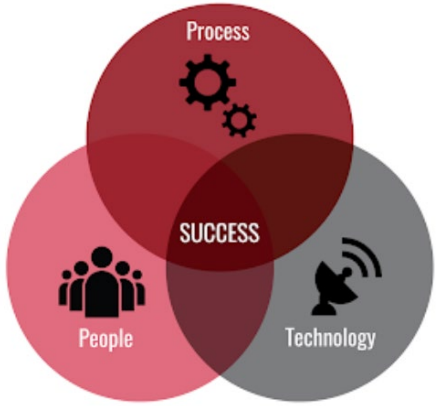
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- What is cybersecurity all about?

People, Process and Technology



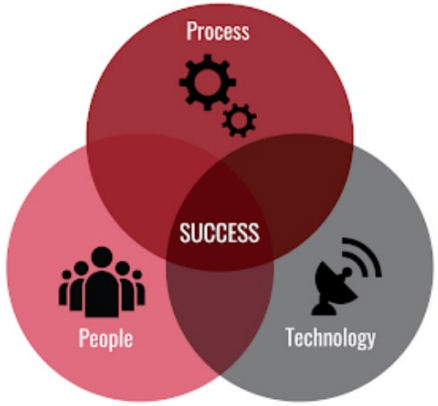
- People - Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

People, Process and Technology (Cont.)



- Process - Organizations must have a framework for how they deal with both attempted and successful cyber attacks.

People, Process and Technology (Cont.)



- Technology - Is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks.

Mitigating Cybersecurity Risks

- AB670: Independent Security Assessment (ISA)
- E-Mail Security Features
- Security Information and Events Management (SIEM)

2021 Accomplishments

Ransomware and Phishing

- There's been a huge increase in the number of ransomware and phishing attacks over the year
- These attacks continue to rise and are getting more dangerous, with cyber criminals aiming to encrypt as much of a corporate network as possible. A single attack can result in cyber criminals making hundreds of thousands or even millions of dollars not to mention the lost of trust in protecting user's information.
- The CalHFA Information Technology Division has been working on protecting our staff and data.

AB670: Independent Security Assessment (ISA)

Why do we need it?

- State of California Requirement
- Mandated by Office of Information Security
- These assessment assist in protecting CalHFA information assets

How was it is being carried out?

- Internal Vulnerability Assessment (Email Phishing)
- External Penetration Testing
- Web Application Testing

What does this get us?

- Detailed Report on observations/findings on 32 control objectives
- Suggested remediation steps for rating less than an “I”

I	P	N

2021 Accomplishments

Email Security Features

- Spoofing prevention
  - DMARC, SPF, DKIM
  - 3rd party e-mail authorization
- Increased security controls
  - SMTP relay enhancement

2021 Accomplishments

Implement a Security Information and Events Management (SIEM)

- A SIEM collects security data from network devices, servers, endpoints and more.
- Bird's- Eye view into our infrastructure.
- On-boarding 24/7 External Security Operations Center (SOC) Monitoring

2021 Accomplishments

Create and Implement Conditional Access Policies for O365 remote use

- Security policies that allow us to manage and monitor activity used to access CalHFA data remotely.

2021 Accomplishments

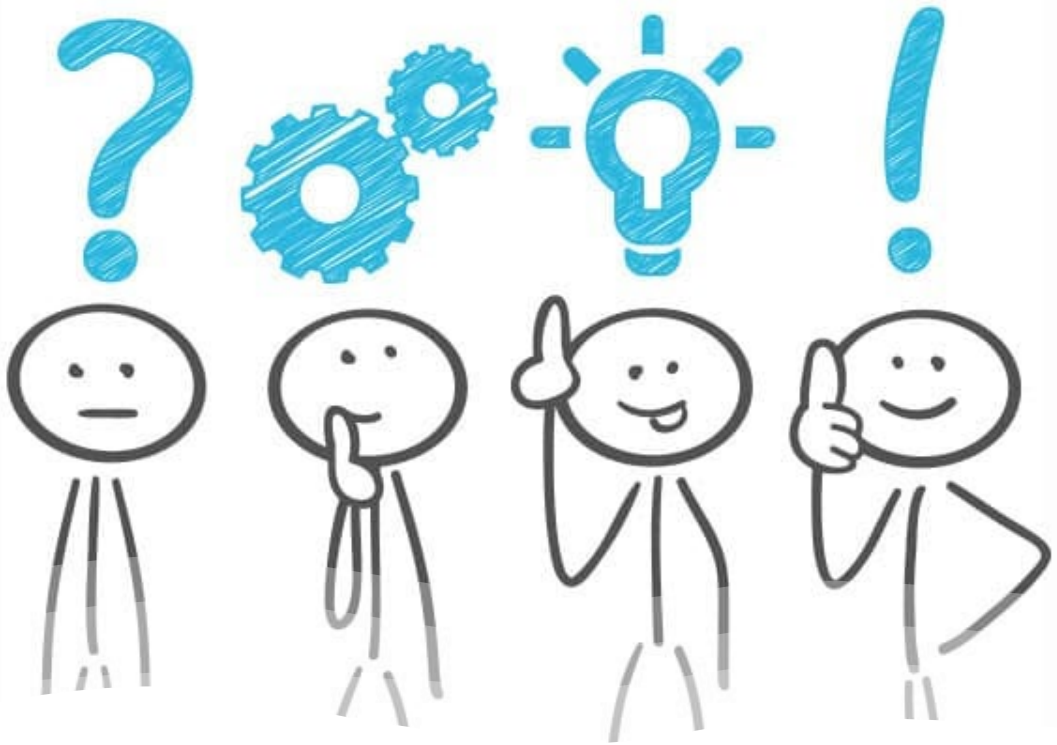
Looking Ahead to 2022

Leverage Existing Security Tools

- With dedicated staff the security group will be able to consistently manage/monitor the digital environment with existing security tools (proactive vs. reactive)

Create and Implement Policies for O365 remote device use

- Security policies that will allow us to manage and monitor our devices used to access CalHFA data.



Questions