

• **LIVE** WEBINAR:

Cybersecurity & Must Do's for Hawaii Employers

Friday, April 22 @ 8:30 - 9:30 am





What you'll learn today

1.

How vulnerable are Hawaii organizations?

2.

How do Cyber Attackers attack?

3.

What can you and your employees do to protect your business, data and people?

How vulnerable are we?



HAWAII CRIME
FBI releases list of top cyber crimes in Hawaii
by: [Chelsea Yee](#)
Posted: Mar 22, 2022 / 03:51 PM HST
Updated: Apr 17, 2022 / 07:08 PM HST

Advertisement

Star Advertiser
Wednesday, April 20, 2022 | Today's Paper | 73°

Advertisement

TOP NEWS

Honolulu Board of Water Supply, Emergency Medical Services report cyberattacks on employee data

By [Star-Advertiser Staff](#) Dec. 13, 2021

UPDATE: 4:15 p.m.

The time-keeping system Honolulu Emergency Medical Services uses for employees was hit by a ransomware attack Sunday night, the third cyber intrusion of county networks since Thursday.

FMS uses the same third-party system from the company Kronos as the Honolulu Board of

Advertisement

SUBSCRIBER FAVORITES

- 1 Police arrest teen for allegedly beating family member to death in Makaha
- 2 Senate accused of 'punitive' funding plan for University of Hawaii
- 3 Holly Shikada confirmed as top law enforcement officer
- 4 Dr. Rudolph B. Puana, brother of Katherine Kealoha, found guilty of distributing oxycodone and fentanyl
- 5 Mega dance company bred culture of sex, silence, dancers say

Shields Up: U.S. officials preparing for potential Russian cyberattacks

60 BY BILL WHITAKER
APRIL 17, 2022 / 6:57 PM / CBS NEWS



Small and Medium Sized Organizations are increasingly at risk...even in Hawaii

Organizations with <100 employees are **350% more likely** to be cyberattacked vs enterprise

Why?

- Lack security expertise & resources
- No contingency plans
- Don't focus on employee education

- *Small businesses account for 43% of cyber attacks*
- *Average cost is \$9,000 per attack*
- *47% of small businesses say they have no understanding of how to protect themselves*



**How do Cyber Attackers
attack?**

**How do we know we've
been attacked?**





Connect with your friend faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

Discover Facebook Mobile

we need your information.

Name:

Surname:

Your email:

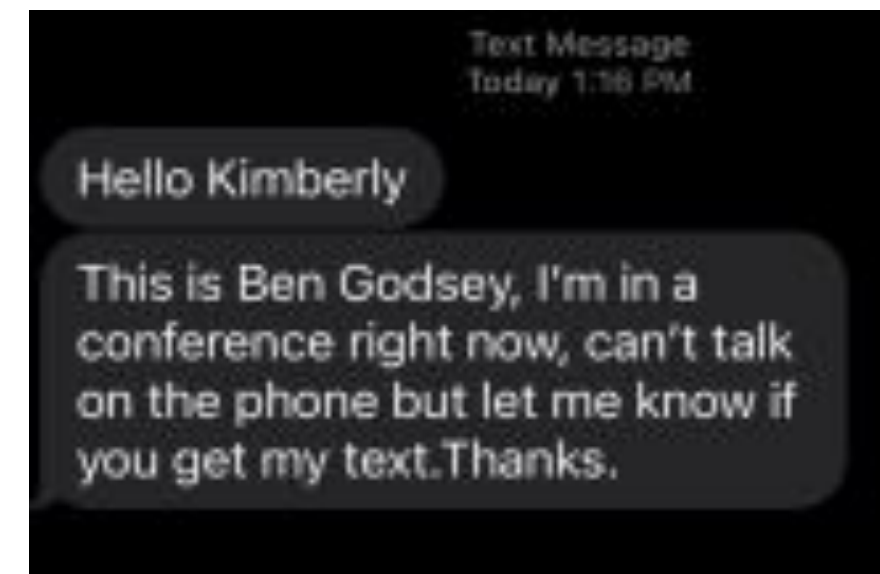
Re-enter your email address:

Password:

Gender:

Date of Birth: Day: Month: Year:

Why do I have to provide my birthday?



Today 07:25


Your Santander Bank Account has been blocked. All services have been withdrawn. Go to <http://santander.onlineupdatesecures.he.net.pk> to reactivate now.

Cyber Attackers attack an organization's weak points

1. Phishing & highly targeted spear-phishing attacks (yes, there's a difference)
2. Outdated operating systems & applications with known vulnerabilities
3. Employee innocence. Without *structured* employee cybersecurity training, cyber attackers enter your company's systems through your employees as they go about their daily work
4. Poor cyber hygiene relating to devices and physical/digital assets

Through many entry points

- Email
- Text
- Websites & Apps
- Phones
- Flash drives
- Computers, laptops, tablets, (game consoles?)
- Employees (whether malicious or just reckless)



What can you and your employees do to protect your organization, your data, your people?



Most common signs you have been breached

1. Your computer suddenly slows down
2. You start losing access to files
3. Weird ad windows start popping up on your screen
4. You get replies to emails that you didn't send
5. A window pops up that says you've been hacked

Six Must Do's to protect your Organization

1. Run operating system and application **patches and updates** on *everything*
2. Give your employees *structured* **cybersecurity training**. Teach them how to identify threats!
3. Use a **password manager** to generate secure passwords and store them safely
4. Enable **multi-factor authentication** (MFA) for an added layer of security if your username/passwords become compromised
5. **Backup your data** (cloud storage and other options...or bring in a pro)
6. Prioritize the **business systems** you need to bring back online first if breached, and know **who to call**

We've been attacked. What do we do?

Immediately

- 1. Shutdown all computers, phones – company, employee**
- 2. Contact your IT and/or cyber security resources**

As soon as possible

- 1. Change passwords**
- 2. Report phishing attacks**
- 3. Isolate critical systems from network and scan**
- 4. Try to retain all data, hardware/drives for forensics**
- 5. Report to FBI**
- 6. Notify customers, vendors of your temporary changes in business operations**

Cyber Security takes specialized expertise

Tap into Hawaii Cyber Experts



Loren Aquino,
CXO,
HI Tech Hui



Attila Seress,
President,
Cylanda



Jeff Saari,
Program Manager,
Ulu HI-Tech



WEBINAR SERIES:

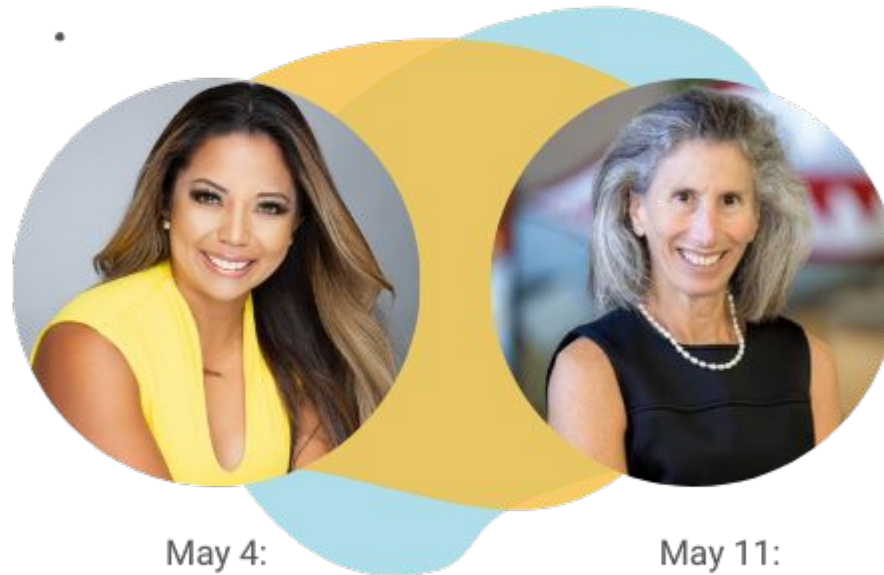
Managing Employee Performance

Wednesday, May 4 and 11 @ 2-3 pm

. . .
. . .
. . .
. . .
. . .

Wednesday, May 4 @ 2-3 pm

Can Your People Execute Your Growth Strategy? How to Coach Them So They Can.



May 4:
Tiera Covington
Owner, Integrated Facility
Services Hawaii

May 11:
Elissa Lines
Executive Director,
Pearl Harbor Aviation Museum

.
.

Wednesday, May 11 @ 2-3 pm

Reskilling Your Staff to Drive Business Transformation

#ASKUSANYTHING

What questions do you have for our experts?





Mahalo to Hawaii's Cyber Experts!



Loren Aquino,
CXO,
HI Tech Hui



Attila Seress,
President,
Cylanda



Jeff Saari,
Program Manager,
Ulu HI-Tech



Mahalo for attending!

