

## **Operations Update**

Plant Operations – Plant operations and treatment were good for the month of June. No credits were used from the treatment basin.

DNR Response to CMAR – Included with this update is the positive response from our DNR Basin Engineer for the 2018 CMAR.

KnowBe4 Security Awareness Training – Due to the vast use of computers used at the Heart of the Valley MSD, it increases the possibility of being exposed to phishing and ransomware attacks. I've included information on a training program that has been set up for all personnel to help become aware of these attacks and try to prevent them from happening. Also included is an article about a recent ransomware attack on a city in Florida.

## **Maintenance Update**

Day Tank Mixer – The day tank mixer has been received and installed.

Laser Flow System Meters – The remaining six Laser Flow meters have been ordered.

HOV Agricultural Land (Grass Buffers) – Have received one quote and waiting for a second.

Variable Frequency Drive Post ATAD- The Power Flex 700 drive for Post ATAD Blower #3 failed. I looked at several different options to replace; new \$10,266 one year warranty, exchange unit \$6,061 two year warranty. Lead time on rebuild options were too long and less of a warranty. Also looked at upgrading to a Power Flex 753 drive but because of space requirements it would not fit in the enclosure. Went with the exchange unit; received the unit and installed, blower back up and running with very little down time.

Allen Bradley Control Logic Power Supply – Received a call one Saturday afternoon just prior to the weekend operator leaving for the day. The plant lost communications to the PLC in the headworks building from all other PLC's in the plant. After some trouble shooting we found that the PLC had lost power and the cause being the control logic power supply. The plant keeps one in stock, which enabled us to replace it and get all equipment running in auto again.

Biostyr Blower – Recently a biostyr blower failed and was more involved than the scope of repairs that plant personnel does. Arranged for an exchange blower unit with Aerzen. The cost for this exchange will be about \$4500.

Kevin Skogman  
Director of Operations & Maintenance

# Compliance Maintenance Annual Report

Heart Of The Valley Metro Sewerage District

Last Updated: Reporting For:

6/12/2019

2018

## DNR Response to Resolution or Owner's Statement

Name of Governing Body or Owner:	<input type="text" value="Heart of the Valley Metropolitan Sewerage District"/>
Date of Resolution or Action Taken:	<input type="text" value="2019-06-11"/>
Resolution Number:	<input type="text" value="184"/>
Date of Submittal:	6/12/2019
<b>ACTIONS SET FORTH BY THE GOVERNING BODY OR OWNER RELATING TO SPECIFIC CMAR SECTIONS (Optional for grade A or B. Required for grade C, D, or F):</b>	
Influent Flow and Loadings: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text"/>	
Effluent Quality: BOD: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text" value="Good effluent BOD quality."/>	
Effluent Quality: TSS: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text" value="Effluent TSS levels are below current limits."/>	
Effluent Quality: Ammonia: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text" value="Good effluent Ammonia quality."/>	
Effluent Quality: Phosphorus: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text" value="Effluent phosphorus levels are below current limits."/>	
Biosolids Quality and Management: Grade = A	
<b>Permittee Response:</b>	
<b>DNR Response:</b>	
<input type="text" value="Biosolids metal quality values are below the high quality limits."/>	
Staffing: Grade = A	

# Compliance Maintenance Annual Report

Heart Of The Valley Metro Sewerage District

Last Updated: Reporting For:  
6/12/2019 2018

**Permittee Response:**

**DNR Response:**

It appears that the preventative maintenance program is well managed.

Operator Certification: Grade = A

**Permittee Response:**

**DNR Response:**

Financial Management: Grade = A

**Permittee Response:**

**DNR Response:**

The equipment replacement fund has a good ending balance and the energy efficiency practices are strong.

Collection Systems: Grade = A

(Regardless of grade, response required for Collection Systems if SSOs were reported)

**Permittee Response:**

**DNR Response:**

The Department recognizes your efforts in controlling I/I in the sanitary sewer collection system. Please continue to address the issues.

**ACTIONS SET FORTH BY THE GOVERNING BODY OR OWNER RELATING TO THE OVERALL GRADE POINT AVERAGE AND ANY GENERAL COMMENTS**

(Optional for G.P.A. greater than or equal to 3.00, required for G.P.A. less than 3.00)

**G.P.A. = 4**

**Permittee Response:**

**DNR G.P.A. Response:**

The facilities appear to be well maintained and operated efficiently.

**DNR CMAR Overall Response:**

Thank you for submitting the Compliance Maintenance Annual Report (CMAR) in a timely manner. The report's G.P.A. shows the dedication of everyone involved in the management and maintenance of the WWTF and the sanitary sewer collection system.

**DNR Reviewer:** Van Gheem, Roy

**Phone:** (920) 662-5191

**Address:** 2984 Shawano Avenue, Green Bay, WI 54313-6727

**Date:** 6/17/2019

## Kevin Skogman

---

FORT LAUDERDALE, Fla. (AP) —

A Florida city agreed to pay \$600,000 in ransom to hackers who took over its computer system, the latest in thousands of attacks worldwide aimed at extorting money from governments and businesses.

The Riviera Beach City Council voted unanimously this week to pay the hackers' demands, believing the Palm Beach suburb had no choice if it wanted to retrieve its records, which the hackers encrypted. The council already voted to spend almost \$1 million on new computers and hardware after hackers captured the city's system three weeks ago. The hackers apparently got into the city's system when an employee clicked on an email link that allowed them to upload malware. Along with the encrypted records, the city had numerous problems including a disabled email system, employees and vendors being paid by check rather than direct deposit and 911 dispatchers being unable to enter calls into the computer. The city says there was no delay in response time.

Spokeswoman Rose Anne Brown said Wednesday that the city of 35,000 residents has been working with outside security consultants, who recommended the ransom be paid. She conceded there are no guarantees that once the hackers received the money they will release the records. The payment is being covered by insurance. The FBI on its website says it "doesn't support" paying off hackers, but Riviera Beach isn't alone: many government agencies and businesses do.

"We are relying on their (the consultants') advice," she said. The hackers demanded payment in the cryptocurrency bitcoin. While it is possible to trace bitcoins as they are spent, the owners of the accounts aren't necessarily known, making it a favored payment method in ransomware attacks.

Numerous governments and businesses have been hit in the United States and worldwide in recent years. Baltimore refused to pay hackers \$76,000 after an attack last month. The U.S. government indicted two Iranians last year for allegedly unleashing more than 200 ransomware attacks, including against the cities of Atlanta and Newark, New Jersey. The men, who have not been arrested, received more than \$6 million in payments and caused \$30 million in damage to computer systems, federal prosecutors have said.

The federal government last year also accused a North Korean programmer of committing the "WannaCry" attack that infected government, bank, factory and hospital computers in 150 countries. He is also believed to have stolen \$81 million from a Bangladesh bank. He also remains in his home country.

The FBI had no comment Wednesday on the Riviera Beach attack, but said 1,493 ransomware attacks were reported last year with victims paying \$3.6 million to hackers — about \$2,400 per attack. Some of those were against individuals.

Tom Holt, a Michigan State University criminal justice professor, said hackers often attack common and known vulnerabilities in computer systems. He said organizations' technology managers need to examine their systems for such flaws and teach their employees not to open suspicious email or click suspect links. The FBI says businesses also need to back up their data regularly on secure computers.

Holt said most attacks originate outside the U.S., making them difficult to police. He said many victims wind up like Riviera Beach: They pay their attacker because it is likely the only way to retrieve lost data.

"They might not pay the initial ransom that was suggested, but they may work with a third-party provider to negotiate the ransom down," Holt said.

He said in almost all cases, the attackers decrypt the computers after payment, allowing the victims to retrieve their data. He said the WannaCry attacks were an exception — the hackers took the money but often didn't release the data. Some private WannaCry decryption attempts were successful.

Copyright 2019 Associated Press. A

Kevin Skogman

Director of Operations and Maintenance

Heart of the Valley Metro. Sew. Dist.

Email: [kevin.skogman@hvmsd.org](mailto:kevin.skogman@hvmsd.org)


PH: 920-766-5731


# Security Awareness Training and Simulated Phishing Platform


Helps you manage the ongoing problem of **social engineering**


## KnowBe4 Security Awareness Training

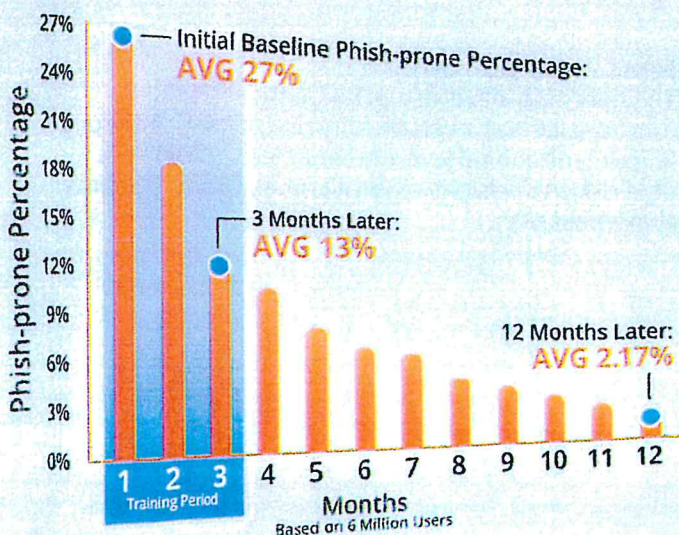
Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

 **Baseline Testing**  
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

 **Train Your Users**  
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

 **Phish Your Users**  
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

 **See the Results**  
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



### The System Really Works

With KnowBe4's massive database, we analyzed 6 million users over the course of 12 months, and our 2018 research uncovered some surprising results. The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 27%.

Fortunately, the data showed that this 27% can be brought down more than half to just 13% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2.17% on average.

See how your company's phish-prone percentage compares to your peers! **Industry Benchmarking** feature included with your subscription.

# Find out How Effective Our Security Awareness Training Is

KnowBe4 is the world's largest integrated platform for awareness training combined with simulated phishing attacks. Join our tens of thousands of customers who have mobilized their end users as a last line of defense.

## KnowBe4 Security Awareness Training Features



### Unlimited Use

We offer three Training Access Levels, giving you access to our content library of 850+ items based on your subscription level. Unlimited access to all phishing features with flexible licensing. No artificial license ceilings and 10% overage allowance. Powerful new features added regularly.



### Engaging, Interactive Browser-based Training

The interactive training gives your users a fresh new learner experience that makes learning fun and engaging. With the optional gamification feature, users can compete against their peers on leaderboards and earn badges while learning how to keep your organization safe from cyber attacks.



### Custom Phishing Templates and Landing Pages

Apart from the thousands of easy-to-use existing templates, you can customize scenarios based on personal information and include simulated attachments to create your own targeted spear phishing campaigns. Each Phishing Email Template can have its own Custom Landing Page, which allows for point-of-failure education.



### Phish Alert Button

KnowBe4's Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis, and deletes the email from the user's inbox to prevent future exposure. All with just one click!



### Social Engineering Indicators

Patented technology turns every simulated phishing email into a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email.



### PhishER

As you phish and train your users they will start reporting potentially dangerous emails to your incident response team. The increase of this email traffic ... can present a new problem! PhishER, is an optional add-on for managing the high volume of messages reported by your users and helps you identify and respond to email threats faster.



### Automated Security Awareness Program (ASAP)

ASAP is a revolutionary new tool for IT professionals, which allows you to create a customized Security Awareness Program for your organization that will help you to implement all the steps needed to create a fully mature training program in just a few minutes!



### User Management

KnowBe4's **Active Directory Integration** allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes. You can also leverage the **Smart Groups** feature to tailor and automate your phishing campaigns, training assignments and remedial learning based on your employees' behavior and user attributes.



### Security Roles

Allows you to define unlimited combinations of level access and administrative ability that you'd like specific user groups to have. With **delegated permissions** you have the ability to limit roles to only display specific data or allow for the phishing, training, and user management of specific groups.



### New! Advanced Reporting Feature

Gives you a collection of 60+ built-in reports that provide a holistic view of your entire organization over time, and expands detailed reporting on key awareness training indicators. Additionally, you can leverage **Reporting APIs** to pull data from your KnowBe4 console. If you manage multiple KnowBe4 accounts, **Roll-up Reporting** makes it easy to select reports and compare results in aggregate across accounts.



### New! Virtual Risk Officer™

The new innovative Virtual Risk Officer (VRO) functionality helps you identify risk at the user, group and organizational level and enables you to make data-driven decisions when it comes to your security awareness plan.