PORT of SAN DIEGO
Waterfront of Opportunity

CYBERATTACK FALL 2018

Crisis Communications Response
CAPIO EPIC Awards Submission

Submitted February 2019

EXECUTIVE SUMMARY

The Port of San Diego was hit by a major cyberattack on September 25, 2018. At the time the attack happened, the Port of San Diego was in the unique position of having been in the process of developing an agency Crisis Communications Plan, which was nearly complete. The cyberattack crisis was the first opportunity to deploy many of the strategies, procedures and tactics envisioned for inclusion in the plan. The Port's Marketing & Communications team worked closely with multiple partners to ensure a coordinated public presence and consistency of information across all channels and partners. The Port successfully communicated with its constituents, the media and nearby residents despite not having immediate access to normal computer systems and while cooperating with an ongoing confidential federal investigation.

I. RESEARCH/PLANNING

At the time the cyberattack hit, Port staff were in the process of creating an agency Crisis Communication Plan (CCP). While the document was not yet finalized, the advanced planning that went into this effort positioned the Port for success in managing crisis communications related to the cyberattack.

During the development of the CCP, several research efforts were implemented to gain insight and feedback on how the Port's staff and Board members could be best prepared to respond to stakeholders in the event of a crisis. These research elements included conducting a media audit; interviewing both internal and external stakeholders; meeting with member cities' communications staff members; and facilitating a Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis. The SWOT analysis was conducted during an internal working session with 30 Port staff, which included meaningful discussions to identify possible threats to the Port and responses to potential crisis scenarios. All the work that went into the draft CCP paid off during the cyberattack.

II. IMPLEMENTATION OVERVIEW

For the purpose of this entry, the period of crisis is defined as the first 10 days of the cyberattack, response and recovery, from September 25, 2018 – October 4, 2018.

The cyberattack on the Port of San Diego was first detected on September 25, 2018. Information Technology staff received multiple reports of computers with all files suddenly frozen. Staff reported that notes were popping up on their computer screens, demanding a form of currency known as Bitcoin. All employees were asked to shut down computers while an investigation was initiated. Port staff immediately contacted the California Office of Emergency Services, the County Office of Emergency Services, the U.S. Coast Guard, Department of Homeland Security and the Federal Bureau of Investigation; and the Port's Information Technology team worked throughout the night to identify what was happening.

By the next morning, it was clear that public safety systems were impacted, and there were also impacts to other business operations of the Port. As background, the Port of San Diego oversees 34 miles of San Diego Bay waterfront in five Port cities including cargo and cruise terminals, hotels, restaurants and marinas. From the Public Information Officer perspective, the first question was: "What is the impact of this cyberattack on the public?" Even though there were many unknowns, it was clear that given the seriousness of the situation, the public needed to be alerted without delay.

Following the procedures outlined in the draft CCP, a cross-departmental team met to consider public-facing statements. In order to be transparent and proactive rather than reactive, and having received no media inquiries thus far, the team decided it was important to notify the media as soon as possible. One challenge was obtaining review and signoff from partner agencies, such as the FBI. Many details were deemed confidential. Given the seriousness and sensitivity of the situation, it was determined that the Port's CEO would be quoted in a statement and would not provide interviews.

Because computers were shut down, Port staff faced technical hurdles in issuing the statement. Fortunately, the Information Technology Department prioritized computers for communications staff. The Port's Public Information Officer was issued a new laptop computer at about noon on September 26, 2018. The statement was issued via the portofsandiego.org website at 1 p.m. on September 26, 2018, as well as via Mailchimp, Twitter, Facebook and LinkedIn.

STATEMENT 1: September 26, 2018 – Port of San Diego Issues Statement on Cybersecurity Incident

“The Port of San Diego has experienced a serious cybersecurity incident that has disrupted the agency’s information technology systems. The Port first received reports of the disruption on Tuesday, September 25, 2018. The Port has mobilized a team of industry experts and local, regional, state and federal partners to minimize impacts and restore system functionality, with priority placed on public safety-related systems. The Harbor Police Department has alternative systems and procedures in place to minimize impacts to public safety. Additionally, we have reported this disruption to the California Office of Emergency Services (Cal OES) and the County of San Diego Office of Emergency Services. Port employees are currently at work but have limited functionality, which may have temporary impacts on services to the public, especially in the areas of park permits, public records requests, and business services. No further information is available at this time; updates will be provided as information is available,” said Port of San Diego CEO Randa Coniglio.

This statement prompted a barrage of media inquiries (none had been received prior to the statement being issued), including four public records requests, and made front-page news in the local newspaper of record, The San Diego Union-Tribune. Communications staff logged 38 media inquiries.

Many machines and systems were shut down as a precaution and remained that way for a week or more. The Port issued three more statements over the 10-day period, each one providing an update.

The next major action in the cyberattack took place November 28, 2018. The Department of Justice/FBI announced two indictments in what was described as a 34-month-long international computer hacking and extortion scheme. The indictment revealed that the Port of San Diego was the final victim among more than 200 public agencies over the 34-month period.

II. RESULTS/EVALUATION

Thanks to advance preparation, including the development of a draft Crisis Communications Plan, the Port’s Crisis Communications Response to the cyberattack was successfully able to balance public safety with the public’s right to know and protect the agency’s reputation along with public confidence in the response. An analysis via the Cision Public Relations media monitoring platform showed that the Port received 1,477 media mentions on news sites and in social media in the first 10 days of the attack. Of those, 83.33 percent were neutral, and only 16.67 percent were categorized as negative, according to Cision.

The Port’s social media channels had significant engagement with posts about the cyberattack, as follows:

- Twitter Impressions: 13,913
- Facebook reach: 3,419
- LinkedIn Impressions: 5,553

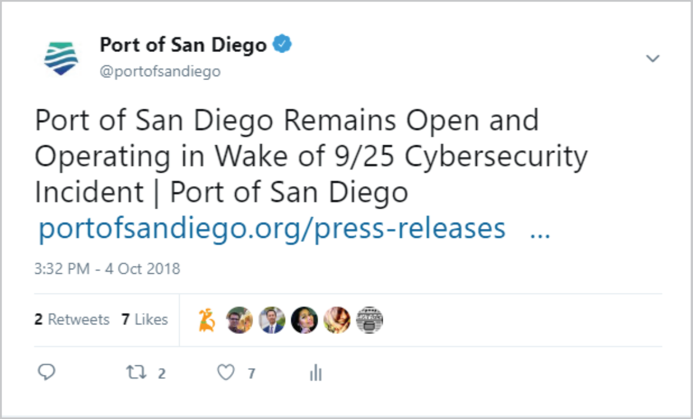
IV. BUDGET INFORMATION

Communication tools and tactics of the crisis communications response included:

Expense	Detail	Amount
Social Media	Facebook (4), Twitter (4), LinkedIn (4)	$0
Website	Portofsandiego.org	$0
Press Releases	MailChimp (4 – Included in Annual Subscription)	$0
Estimated Staff Time*	140 Hours, Est. Hourly Avg. $60	$8,400
Response Cost Total	**(Hard and Soft Cost)**	**$8,400**

(*Includes Port Executives, Communications Director, Public Information Officer, Multi-Media Specialist as well as IT, Legal and Law Enforcement Subject Matter Experts on-staff)

PORT SOCIAL MEDIA SAMPLING

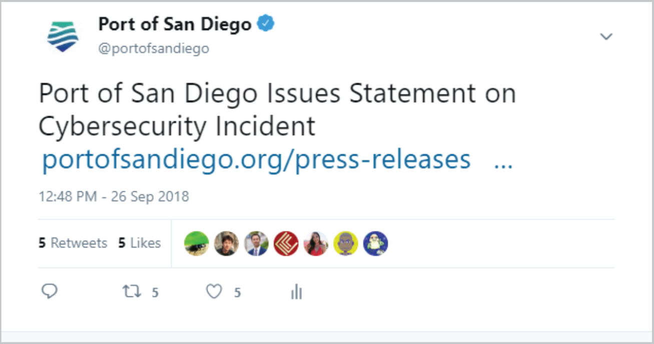


Port of San Diego
@portofsandiego

Port of San Diego Remains Open and Operating in Wake of 9/25 Cybersecurity Incident | Port of San Diego
portofsandiego.org/press-releases …

3:32 PM - 4 Oct 2018

2 Retweets 7 Likes

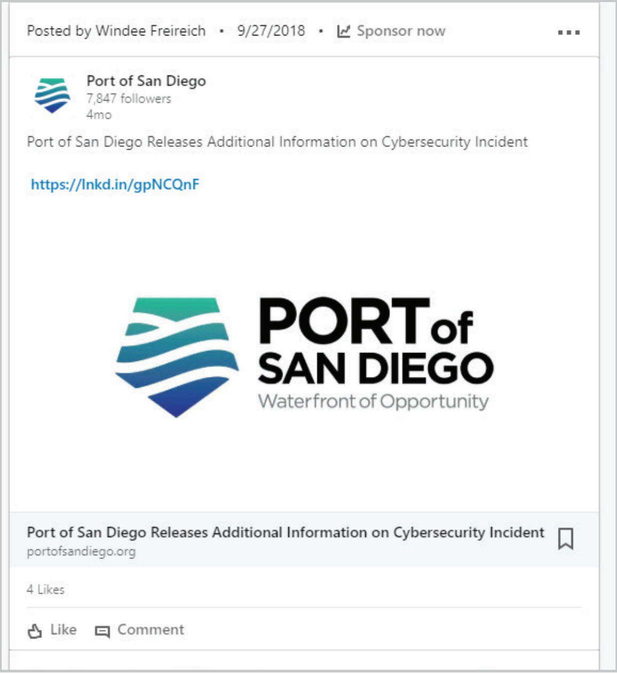


Port of San Diego
@portofsandiego

Port of San Diego Issues Statement on Cybersecurity Incident
portofsandiego.org/press-releases …

12:48 PM - 26 Sep 2018

5 Retweets 5 Likes



Posted by Windee Freireich • 9/27/2018 • Sponsor now

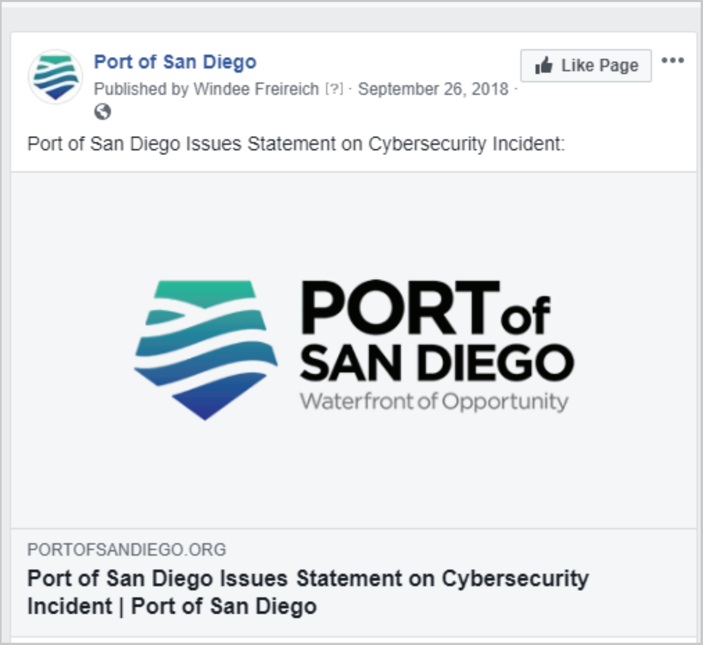
Port of San Diego
7,847 followers
4mo

Port of San Diego Releases Additional Information on Cybersecurity Incident

https://lnkd.in/gpNCQnF

Port of San Diego Releases Additional Information on Cybersecurity Incident
portofsandiego.org

4 Likes

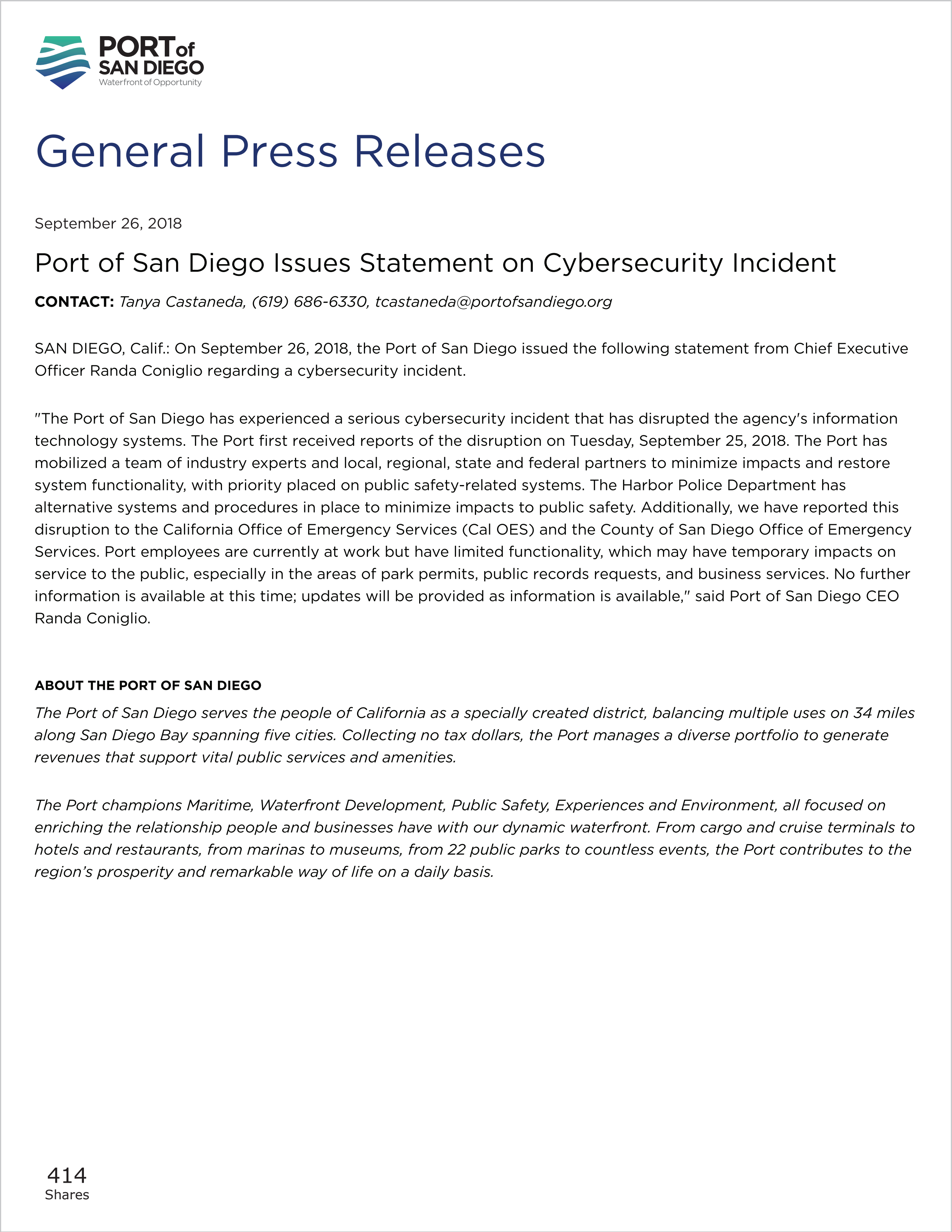


Port of San Diego
Published by Windee Freireich [?] · September 26, 2018 ·

Port of San Diego Issues Statement on Cybersecurity Incident:

PORTOFSANDIEGO.ORG
Port of San Diego Issues Statement on Cybersecurity Incident | Port of San Diego

PRESS STATEMENTS & RELEASES



General Press Releases

September 26, 2018

Port of San Diego Issues Statement on Cybersecurity Incident

CONTACT: *Tanya Castaneda, (619) 686-6330, tcastaneda@portofsandiego.org*

SAN DIEGO, Calif.: On September 26, 2018, the Port of San Diego issued the following statement from Chief Executive Officer Randa Coniglio regarding a cybersecurity incident.

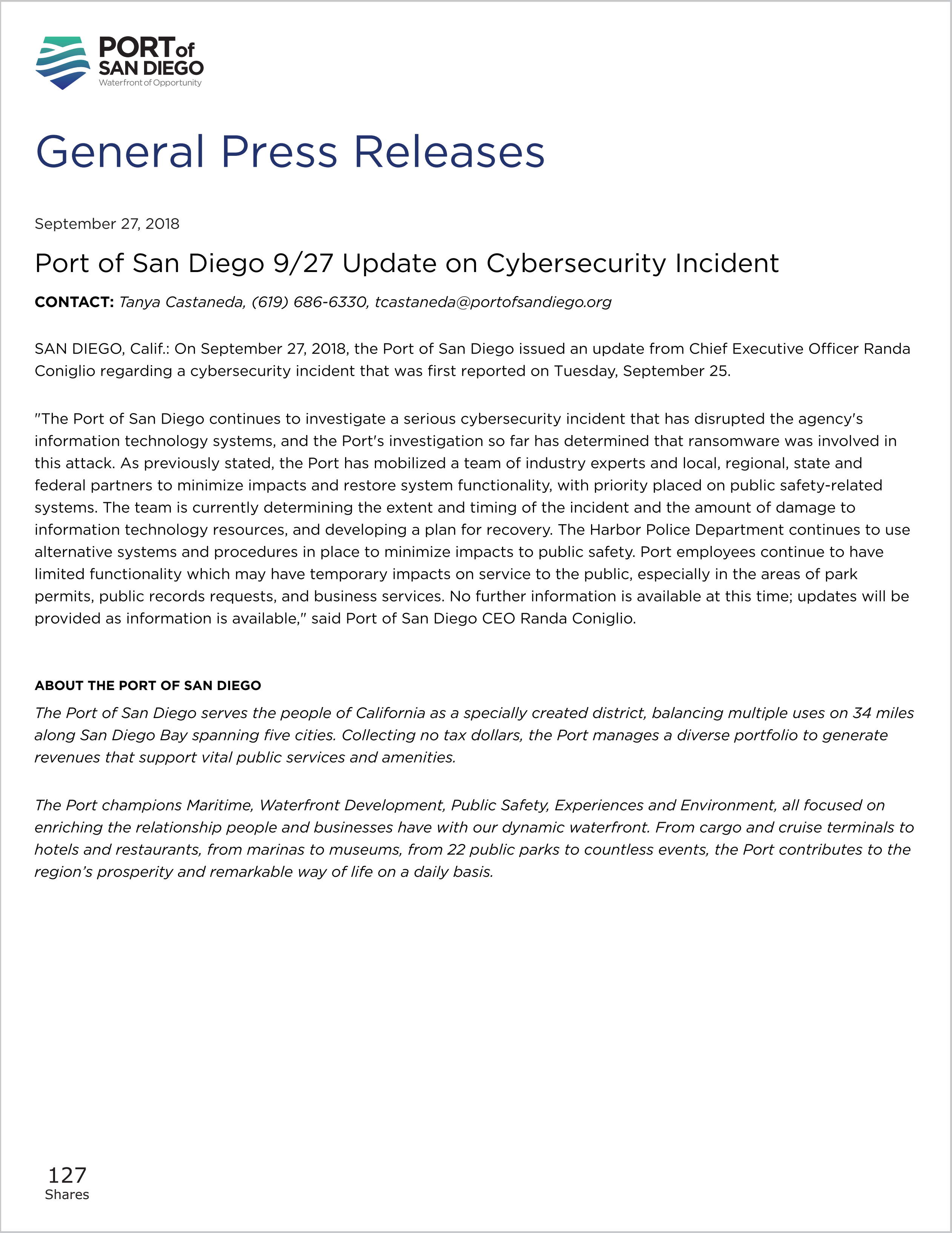
"The Port of San Diego has experienced a serious cybersecurity incident that has disrupted the agency's information technology systems. The Port first received reports of the disruption on Tuesday, September 25, 2018. The Port has mobilized a team of industry experts and local, regional, state and federal partners to minimize impacts and restore system functionality, with priority placed on public safety-related systems. The Harbor Police Department has alternative systems and procedures in place to minimize impacts to public safety. Additionally, we have reported this disruption to the California Office of Emergency Services (Cal OES) and the County of San Diego Office of Emergency Services. Port employees are currently at work but have limited functionality, which may have temporary impacts on service to the public, especially in the areas of park permits, public records requests, and business services. No further information is available at this time; updates will be provided as information is available," said Port of San Diego CEO Randa Coniglio.

ABOUT THE PORT OF SAN DIEGO

The Port of San Diego serves the people of California as a specially created district, balancing multiple uses on 34 miles along San Diego Bay spanning five cities. Collecting no tax dollars, the Port manages a diverse portfolio to generate revenues that support vital public services and amenities.

The Port champions Maritime, Waterfront Development, Public Safety, Experiences and Environment, all focused on enriching the relationship people and businesses have with our dynamic waterfront. From cargo and cruise terminals to hotels and restaurants, from marinas to museums, from 22 public parks to countless events, the Port contributes to the region's prosperity and remarkable way of life on a daily basis.

414
Shares



General Press Releases

September 27, 2018

Port of San Diego 9/27 Update on Cybersecurity Incident

CONTACT: *Tanya Castaneda, (619) 686-6330, tcastaneda@portofsandiego.org*

SAN DIEGO, Calif.: On September 27, 2018, the Port of San Diego issued an update from Chief Executive Officer Randa Coniglio regarding a cybersecurity incident that was first reported on Tuesday, September 25.

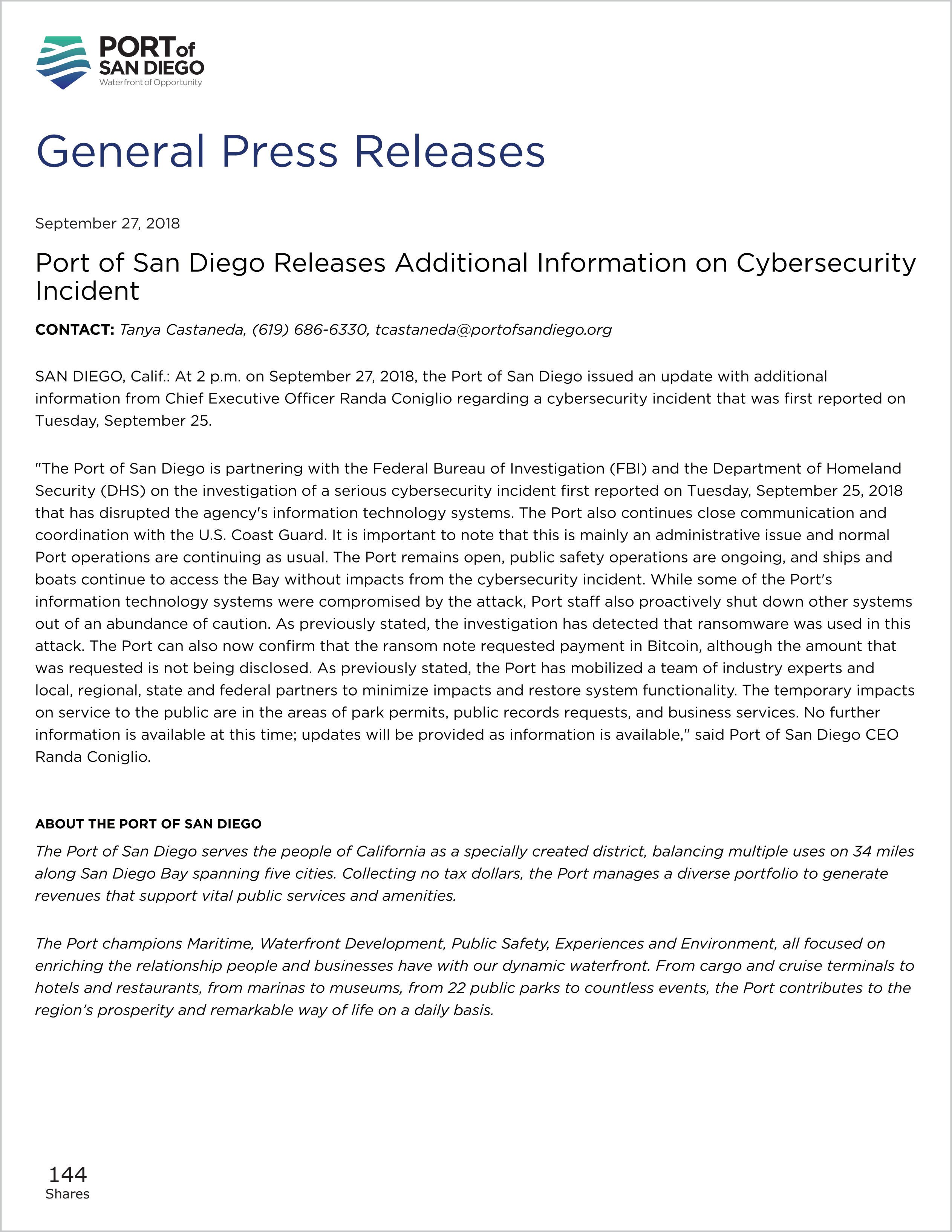
"The Port of San Diego continues to investigate a serious cybersecurity incident that has disrupted the agency's information technology systems, and the Port's investigation so far has determined that ransomware was involved in this attack. As previously stated, the Port has mobilized a team of industry experts and local, regional, state and federal partners to minimize impacts and restore system functionality, with priority placed on public safety-related systems. The team is currently determining the extent and timing of the incident and the amount of damage to information technology resources, and developing a plan for recovery. The Harbor Police Department continues to use alternative systems and procedures in place to minimize impacts to public safety. Port employees continue to have limited functionality which may have temporary impacts on service to the public, especially in the areas of park permits, public records requests, and business services. No further information is available at this time; updates will be provided as information is available," said Port of San Diego CEO Randa Coniglio.

ABOUT THE PORT OF SAN DIEGO

The Port of San Diego serves the people of California as a specially created district, balancing multiple uses on 34 miles along San Diego Bay spanning five cities. Collecting no tax dollars, the Port manages a diverse portfolio to generate revenues that support vital public services and amenities.

The Port champions Maritime, Waterfront Development, Public Safety, Experiences and Environment, all focused on enriching the relationship people and businesses have with our dynamic waterfront. From cargo and cruise terminals to hotels and restaurants, from marinas to museums, from 22 public parks to countless events, the Port contributes to the region's prosperity and remarkable way of life on a daily basis.

127
Shares



General Press Releases

September 27, 2018

Port of San Diego Releases Additional Information on Cybersecurity Incident

CONTACT: *Tanya Castaneda, (619) 686-6330, tcastaneda@portofsandiego.org*

SAN DIEGO, Calif.: At 2 p.m. on September 27, 2018, the Port of San Diego issued an update with additional information from Chief Executive Officer Randa Coniglio regarding a cybersecurity incident that was first reported on Tuesday, September 25.

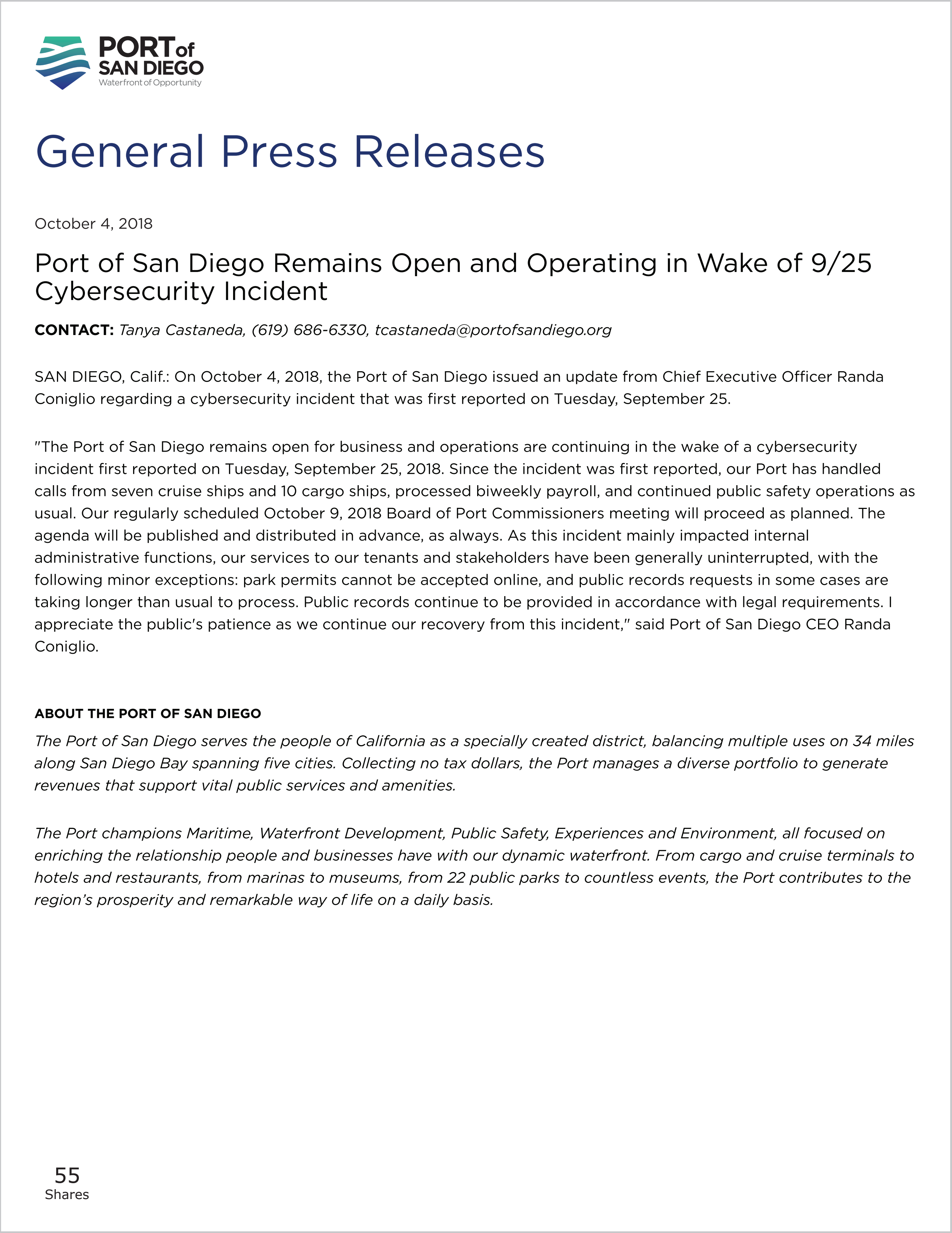
"The Port of San Diego is partnering with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) on the investigation of a serious cybersecurity incident first reported on Tuesday, September 25, 2018 that has disrupted the agency's information technology systems. The Port also continues close communication and coordination with the U.S. Coast Guard. It is important to note that this is mainly an administrative issue and normal Port operations are continuing as usual. The Port remains open, public safety operations are ongoing, and ships and boats continue to access the Bay without impacts from the cybersecurity incident. While some of the Port's information technology systems were compromised by the attack, Port staff also proactively shut down other systems out of an abundance of caution. As previously stated, the investigation has detected that ransomware was used in this attack. The Port can also now confirm that the ransom note requested payment in Bitcoin, although the amount that was requested is not being disclosed. As previously stated, the Port has mobilized a team of industry experts and local, regional, state and federal partners to minimize impacts and restore system functionality. The temporary impacts on service to the public are in the areas of park permits, public records requests, and business services. No further information is available at this time; updates will be provided as information is available," said Port of San Diego CEO Randa Coniglio.

ABOUT THE PORT OF SAN DIEGO

The Port of San Diego serves the people of California as a specially created district, balancing multiple uses on 34 miles along San Diego Bay spanning five cities. Collecting no tax dollars, the Port manages a diverse portfolio to generate revenues that support vital public services and amenities.

The Port champions Maritime, Waterfront Development, Public Safety, Experiences and Environment, all focused on enriching the relationship people and businesses have with our dynamic waterfront. From cargo and cruise terminals to hotels and restaurants, from marinas to museums, from 22 public parks to countless events, the Port contributes to the region's prosperity and remarkable way of life on a daily basis.

144
Shares



PORT of SAN DIEGO
Waterfront of Opportunity

General Press Releases

October 4, 2018

Port of San Diego Remains Open and Operating in Wake of 9/25 Cybersecurity Incident

CONTACT: *Tanya Castaneda, (619) 686-6330, tcastaneda@portofsandiego.org*

SAN DIEGO, Calif.: On October 4, 2018, the Port of San Diego issued an update from Chief Executive Officer Randa Coniglio regarding a cybersecurity incident that was first reported on Tuesday, September 25.

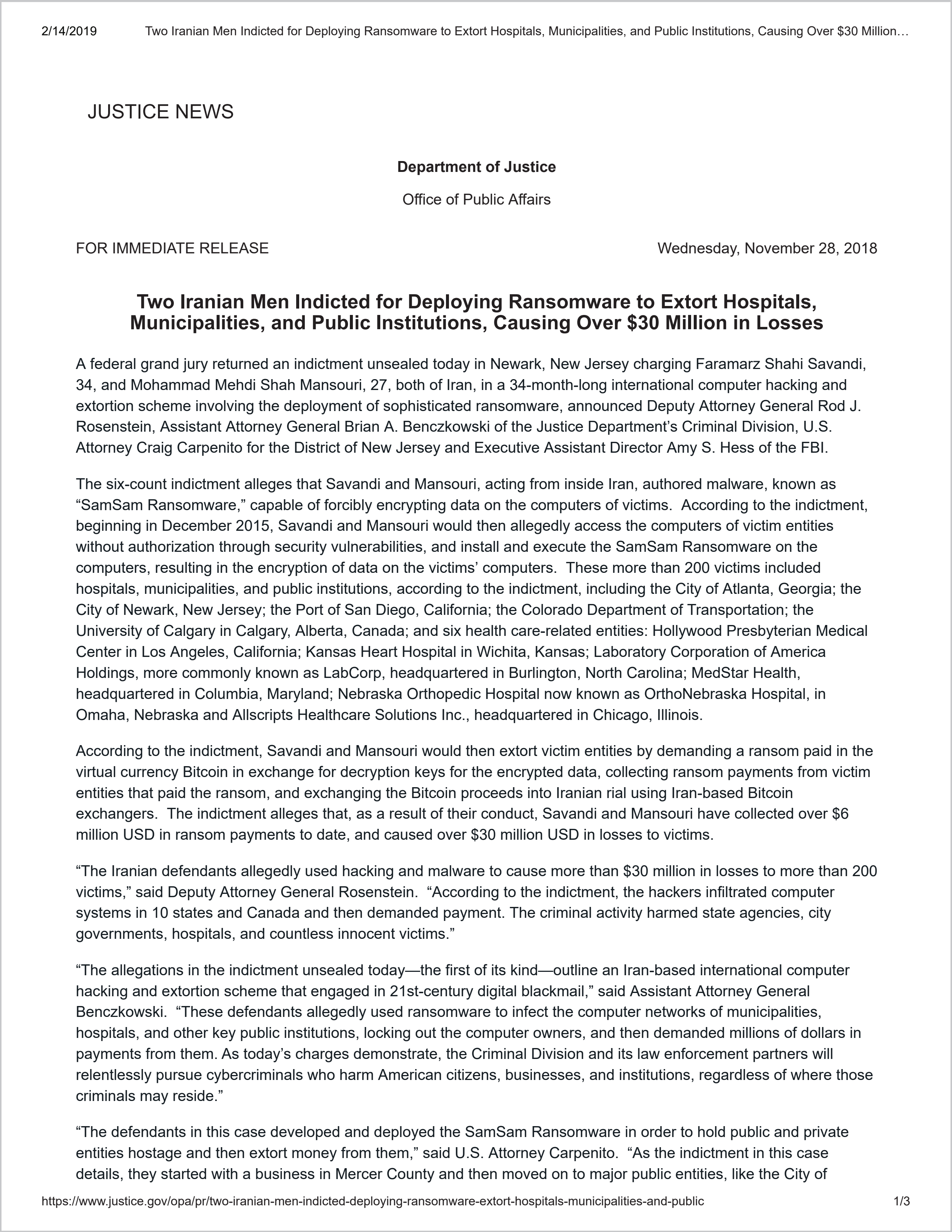
"The Port of San Diego remains open for business and operations are continuing in the wake of a cybersecurity incident first reported on Tuesday, September 25, 2018. Since the incident was first reported, our Port has handled calls from seven cruise ships and 10 cargo ships, processed biweekly payroll, and continued public safety operations as usual. Our regularly scheduled October 9, 2018 Board of Port Commissioners meeting will proceed as planned. The agenda will be published and distributed in advance, as always. As this incident mainly impacted internal administrative functions, our services to our tenants and stakeholders have been generally uninterrupted, with the following minor exceptions: park permits cannot be accepted online, and public records requests in some cases are taking longer than usual to process. Public records continue to be provided in accordance with legal requirements. I appreciate the public's patience as we continue our recovery from this incident," said Port of San Diego CEO Randa Coniglio.

ABOUT THE PORT OF SAN DIEGO

The Port of San Diego serves the people of California as a specially created district, balancing multiple uses on 34 miles along San Diego Bay spanning five cities. Collecting no tax dollars, the Port manages a diverse portfolio to generate revenues that support vital public services and amenities.

The Port champions Maritime, Waterfront Development, Public Safety, Experiences and Environment, all focused on enriching the relationship people and businesses have with our dynamic waterfront. From cargo and cruise terminals to hotels and restaurants, from marinas to museums, from 22 public parks to countless events, the Port contributes to the region's prosperity and remarkable way of life on a daily basis.

55
Shares



2/14/2019 Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million…

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, November 28, 2018

Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses

A federal grand jury returned an indictment unsealed today in Newark, New Jersey charging Faramarz Shahi Savandi, 34, and Mohammad Mehdi Shah Mansouri, 27, both of Iran, in a 34-month-long international computer hacking and extortion scheme involving the deployment of sophisticated ransomware, announced Deputy Attorney General Rod J. Rosenstein, Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Craig Carpenito for the District of New Jersey and Executive Assistant Director Amy S. Hess of the FBI.

The six-count indictment alleges that Savandi and Mansouri, acting from inside Iran, authored malware, known as "SamSam Ransomware," capable of forcibly encrypting data on the computers of victims. According to the indictment, beginning in December 2015, Savandi and Mansouri would then allegedly access the computers of victim entities without authorization through security vulnerabilities, and install and execute the SamSam Ransomware on the computers, resulting in the encryption of data on the victims' computers. These more than 200 victims included hospitals, municipalities, and public institutions, according to the indictment, including the City of Atlanta, Georgia; the City of Newark, New Jersey; the Port of San Diego, California; the Colorado Department of Transportation; the University of Calgary in Calgary, Alberta, Canada; and six health care-related entities: Hollywood Presbyterian Medical Center in Los Angeles, California; Kansas Heart Hospital in Wichita, Kansas; Laboratory Corporation of America Holdings, more commonly known as LabCorp, headquartered in Burlington, North Carolina; MedStar Health, headquartered in Columbia, Maryland; Nebraska Orthopedic Hospital now known as OrthoNebraska Hospital, in Omaha, Nebraska and Allscripts Healthcare Solutions Inc., headquartered in Chicago, Illinois.

According to the indictment, Savandi and Mansouri would then extort victim entities by demanding a ransom paid in the virtual currency Bitcoin in exchange for decryption keys for the encrypted data, collecting ransom payments from victim entities that paid the ransom, and exchanging the Bitcoin proceeds into Iranian rial using Iran-based Bitcoin exchangers. The indictment alleges that, as a result of their conduct, Savandi and Mansouri have collected over $6 million USD in ransom payments to date, and caused over $30 million USD in losses to victims.

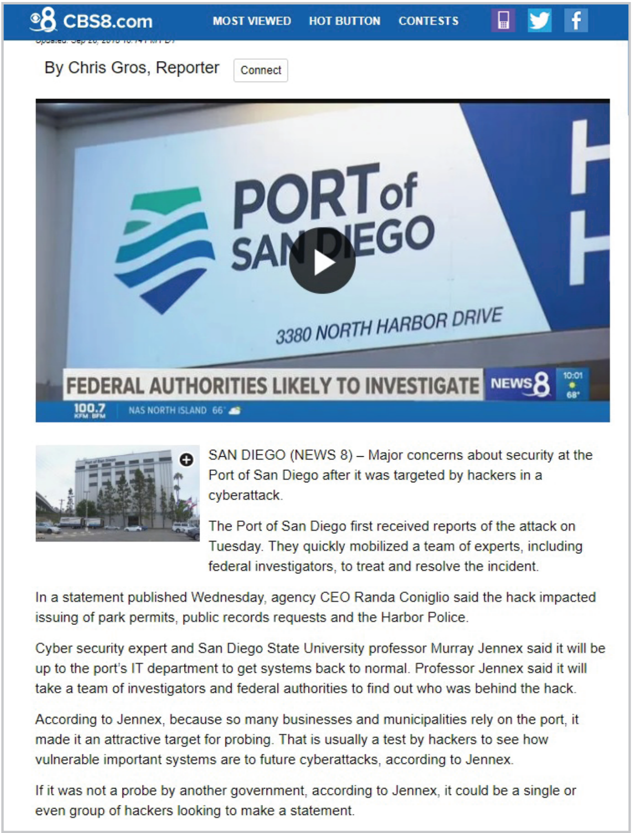
"The Iranian defendants allegedly used hacking and malware to cause more than $30 million in losses to more than 200 victims," said Deputy Attorney General Rosenstein. "According to the indictment, the hackers infiltrated computer systems in 10 states and Canada and then demanded payment. The criminal activity harmed state agencies, city governments, hospitals, and countless innocent victims."

"The allegations in the indictment unsealed today—the first of its kind—outline an Iran-based international computer hacking and extortion scheme that engaged in 21st-century digital blackmail," said Assistant Attorney General Benczkowski. "These defendants allegedly used ransomware to infect the computer networks of municipalities, hospitals, and other key public institutions, locking out the computer owners, and then demanded millions of dollars in payments from them. As today's charges demonstrate, the Criminal Division and its law enforcement partners will relentlessly pursue cybercriminals who harm American citizens, businesses, and institutions, regardless of where those criminals may reside."

"The defendants in this case developed and deployed the SamSam Ransomware in order to hold public and private entities hostage and then extort money from them," said U.S. Attorney Carpenito. "As the indictment in this case details, they started with a business in Mercer County and then moved on to major public entities, like the City of

https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public 1/3

NEWS COVERAGE SAMPLING



By Chris Gros, Reporter

SAN DIEGO (NEWS 8) – Major concerns about security at the Port of San Diego after it was targeted by hackers in a cyberattack.

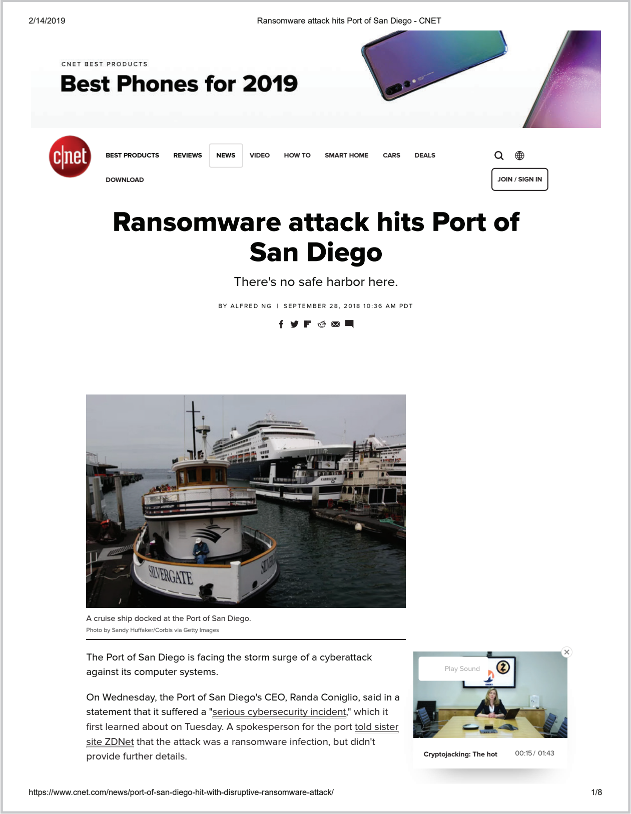
The Port of San Diego first received reports of the attack on Tuesday. They quickly mobilized a team of experts, including federal investigators, to treat and resolve the incident.

In a statement published Wednesday, agency CEO Randa Coniglio said the hack impacted issuing of park permits, public records requests and the Harbor Police.

Cyber security expert and San Diego State University professor Murray Jennex said it will be up to the port's IT department to get systems back to normal. Professor Jennex said it will take a team of investigators and federal authorities to find out who was behind the hack.

According to Jennex, because so many businesses and municipalities rely on the port, it made it an attractive target for probing. That is usually a test by hackers to see how vulnerable important systems are to future cyberattacks, according to Jennex.

If it was not a probe by another government, according to Jennex, it could be a single or even group of hackers looking to make a statement.



2/14/2019 Ransomware attack hits Port of San Diego - CNET

Ransomware attack hits Port of San Diego

There's no safe harbor here.

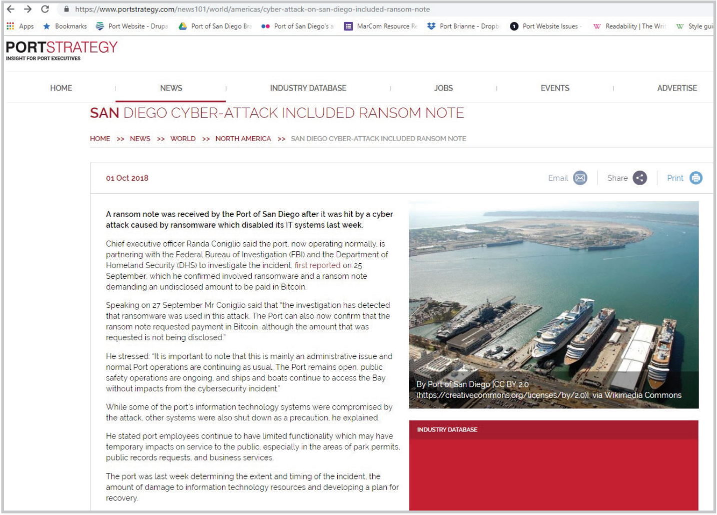
BY ALFRED NG | SEPTEMBER 28, 2018 10:36 AM PDT

A cruise ship docked at the Port of San Diego.
Photo by Sandy Huffaker/Corbis via Getty Images

The Port of San Diego is facing the storm surge of a cyberattack against its computer systems.

On Wednesday, the Port of San Diego's CEO, Randa Coniglio, said in a statement that it suffered a "serious cybersecurity incident," which it first learned about on Tuesday. A spokesperson for the port told sister site ZDNet that the attack was a ransomware infection, but didn't provide further details.

https://www.cnet.com/news/port-of-san-diego-hit-with-disruptive-ransomware-attack/ 1/8



SAN DIEGO CYBER-ATTACK INCLUDED RANSOM NOTE

01 Oct 2018

A ransom note was received by the Port of San Diego after it was hit by a cyber attack caused by ransomware which disabled its IT systems last week.

Chief executive officer Randa Coniglio said the port, now operating normally, is partnering with the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) to investigate the incident, first reported on 25 September, which he confirmed involved ransomware and a ransom note demanding an undisclosed amount to be paid in Bitcoin.

Speaking on 27 September Mr Coniglio said that "the investigation has detected that ransomware was used in this attack. The Port can also now confirm that the ransom note requested payment in Bitcoin, although the amount that was requested is not being disclosed."

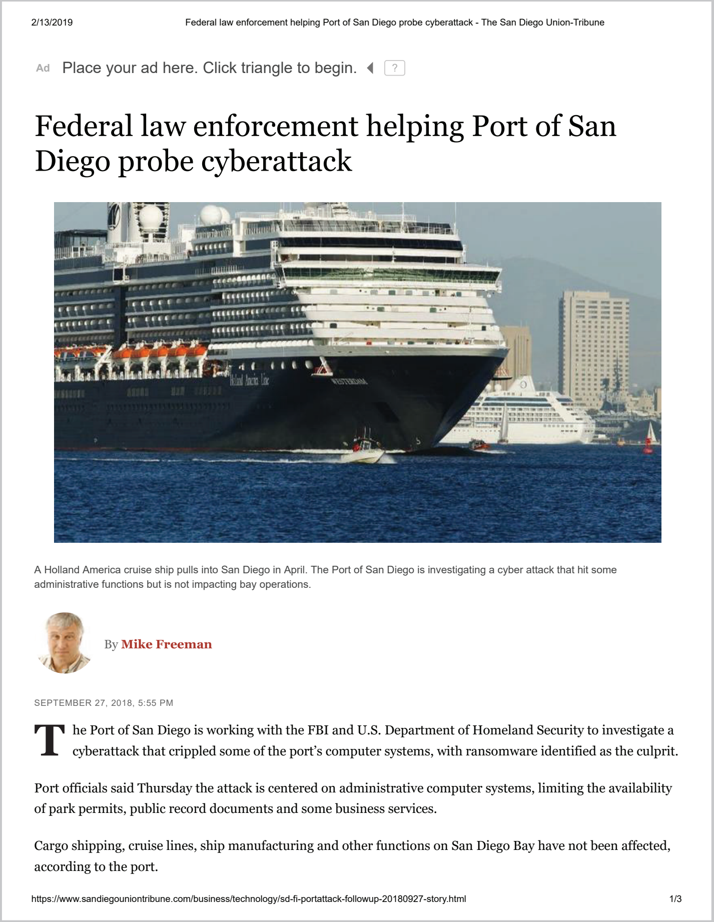
He stressed: "It is important to note that this is mainly an administrative issue and normal Port operations are continuing as usual. The Port remains open, public safety operations are ongoing, and ships and boats continue to access the Bay without impacts from the cybersecurity incident."

While some of the port's information technology systems were compromised by the attack, other systems were also shut down as a precaution, he explained.

He stated port employees continue to have limited functionality which may have temporary impacts on service to the public, especially in the areas of park permits, public records requests, and business services.

The port was last week determining the extent and timing of the incident, the amount of damage to information technology resources and developing a plan for recovery.

By Port of San Diego [CC BY 2.0 (https://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons



2/13/2019 Federal law enforcement helping Port of San Diego probe cyberattack - The San Diego Union-Tribune

Federal law enforcement helping Port of San Diego probe cyberattack

A Holland America cruise ship pulls into San Diego in April. The Port of San Diego is investigating a cyber attack that hit some administrative functions but is not impacting bay operations.

By Mike Freeman

SEPTEMBER 27, 2018, 5:55 PM

The Port of San Diego is working with the FBI and U.S. Department of Homeland Security to investigate a cyberattack that crippled some of the port's computer systems, with ransomware identified as the culprit.

Port officials said Thursday the attack is centered on administrative computer systems, limiting the availability of park permits, public record documents and some business services.

Cargo shipping, cruise lines, ship manufacturing and other functions on San Diego Bay have not been affected, according to the port.

https://www.sandiegouniontribune.com/business/technology/sd-fi-portattack-followup-20180927-story.html 1/3