Cybersecurity Risk Management

City of Ormond Beach

Managing a Breach

ORMOND BEACH OBSERVER FRIDAY, OCT. 13, 2017 4 years ago

Ormond Beach shuts down online utility billing payment system due to potential breach

SHARE COMMENTS 0

Almost 200 customers have notified the city of fraudulent activity on their credit cards.

Looking back in our database, the City of Ormond Beach, FL experienced a similar incident with their Click2Gov system in October 2017. Like Oxnard, it was a credit card issuer that first traced the issue back to Ormond Beach utility payment system, alerting them of the problem on October 11. This, despite the fact that customers had been reporting fraudulent charges they believed to be linked to the City since September 22nd. Ultimately, cards used for payment between approximately mid-September 2017 and October 4, 2017, when the city opted to shut down their system, may have been compromised.

Ormond Beach Investigating Potential Online Utility Payment Security Breach

Posted Friday, October 13, 2017 1:41 pm

Ormond Beach, FL - The City of Ormond Beach is investigating a potential security breach after at least 175 customers reported fraudulent activity on their credit cards after paying their utility bills using the City's online bill paying system. The City partners with a web

gt government technology

Special: Remote Work AI Cloud Cybersecurity Education

CYBERSECURITY

Thousands Exposed in Municipal Website Breaches

Earlier this month, news broke that Wellington, Fla., had sensitive payment information stolen through a billing vendor. Now, it appears the city was not alone.

Adobe Acrobat Sign Secure d signature

Stay or go?

In Ormond Beach, officials already planned to switch to a new payment processing vendor before a customer called in September to report a fraudulent charge on her credit card that was made after she paid her utility bill, information technology director Ned Huhta said.

The city had been with Superion since 1988, and officials felt it was time for a change. "It's been a good run, but they just haven't been as nimble as some of the other vendors," he said.

Officials chose Tyler Technologies — the same vendor Wellington selected last year when it decided to change bill-pay vendors as well. While Ormond Beach is closer to completing its transition to Tyler, Wellington kicked off a three-year migration process Jan. 1.

The customer who raised a red flag for Ormond Beach was one of about 250 utilities customers hit by what that city still calls "a potential breach," having found no "smoking gun" to point to an actual hack, Huhta said.

THE DAYTONA BEACH NEWS-JOURNAL

[News] Sports Entertainment Lifestyle Opinion USA TODAY Obituaries E-Edition Legals

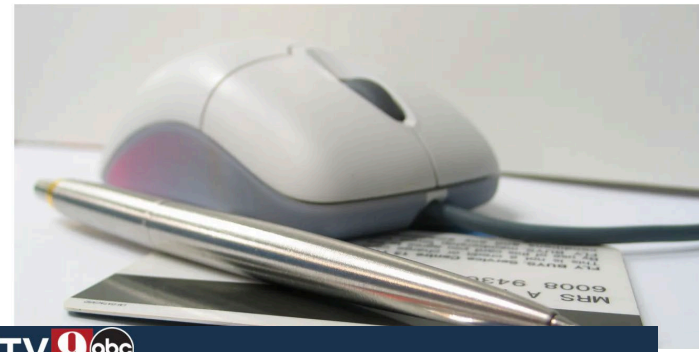
CRIME

Ormond breach? Utility customers see fraudulent charges

Katie Kustura katie.kustura@news-jrnl.com

Published 6:14 p.m. ET Oct. 12, 2017 | **Updated 7:14 a.m. ET Oct. 13, 2017**

View Comments

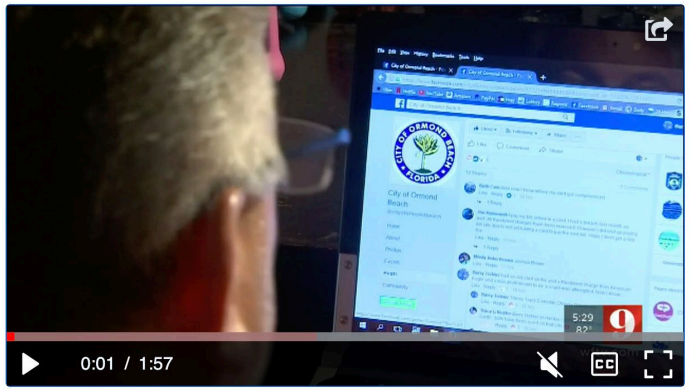


WFTV 9 abc

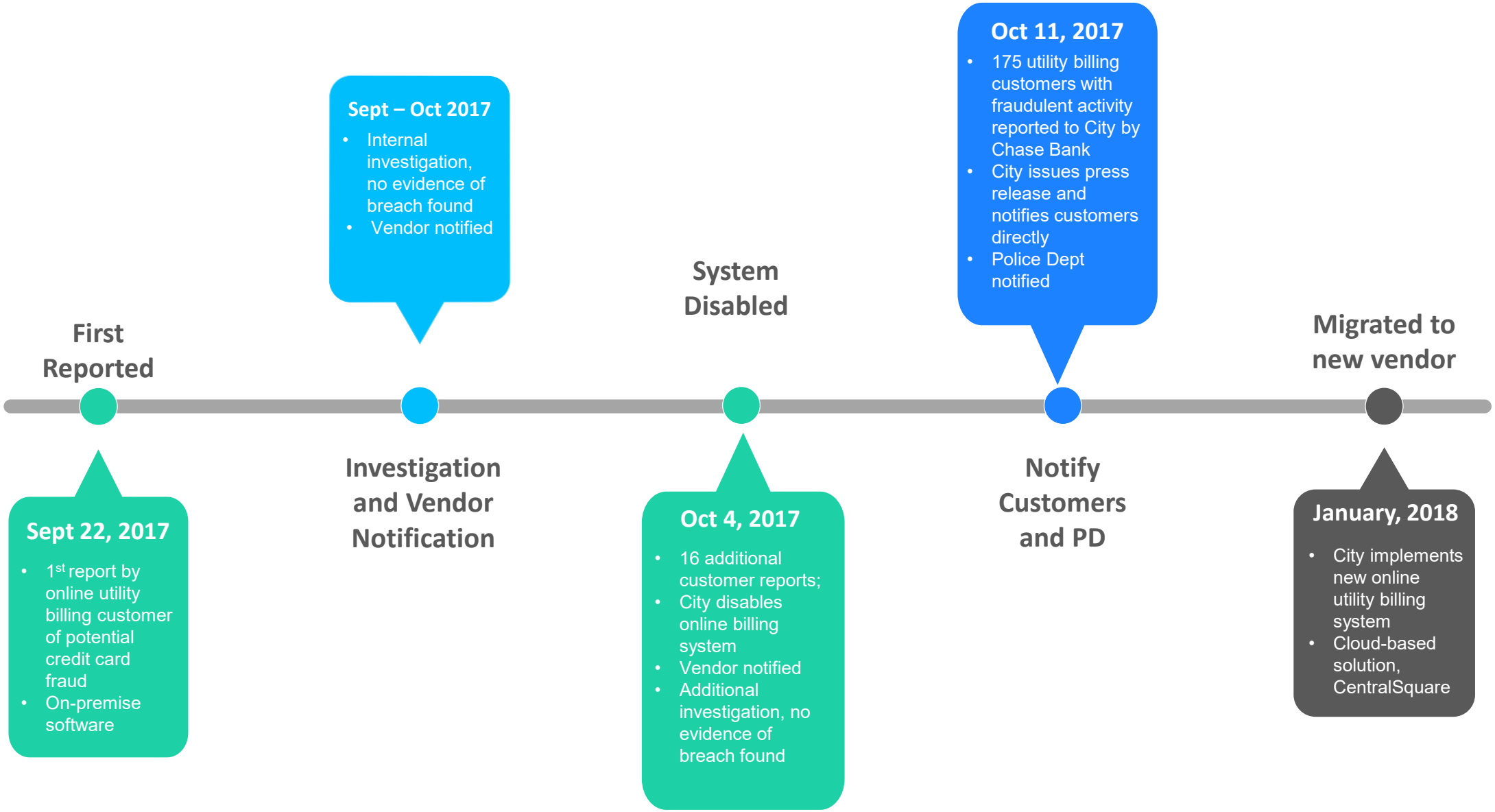
NEWS WEATHER EYE ON THE TROPICS TRAFFIC SPORTS VIDEO 9 FAMILY CONNECTION TH

BREAKING NEWS | Kentucky flooding: Death toll rises to 37, hundreds of people still missing

City of Ormond Beach investigating possible cyberbreach



Superion Click2Gov Incident



Incident Response

2017 Incident Response

Assess Incident

- Immediately initiate internal investigation of potential breach and determine scope

Gather Information

- Internal Team: City Manager, IT, Finance, Police, Vendors
- External Team: local cities, state and federal agencies

Communication

- Customers
  - Include action steps
- Elected Officials
- Media
- Vendors

Additional Best Practices

Assess Incident

- Consider breach in absence of direct evidence
- Reduce time between report and remedial action

Gather Information

- Public Information Officer: data mining and monitoring

Communication

- Customers
  - Early and often to increase transparency
- Staff
  - Training opportunity
- Media
  - Include social media
- Cybersecurity insurance carrier

Prioritizing Cybersecurity

Why Prioritize:

Governments are Primary Targets

Vulnerabilities:

- Inadequate IT security expenditures
  - Equipment
  - Staff training
- Internal processes make it difficult to keep pace with digital evolution
- Entrenched legacy infrastructure
- Updates and patches out of date
- Financial rewards*

Bad actors exploit disruption caused by pandemic:

- Demand for governments to quickly adapt
- New remote work environment
- Expectation of online access to services

44%

of global ransomware attacks in 2020 targeted municipalities

New legislation

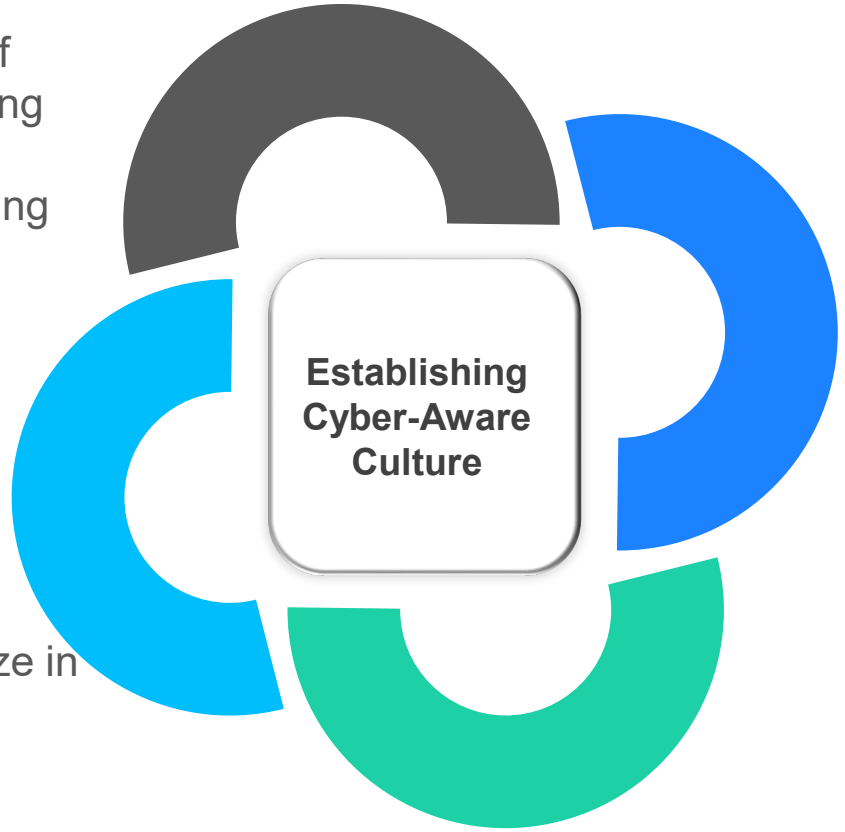
- Requires best practices
- Must close gaps

How to Prioritize:

Mitigating Risk

Staffing

- Invest in knowledgeable IT staff
- Support IT education and training
- Separate cybersecurity officer
- Frequent user awareness training



Policies and Procedures

- Implement least privilege
- Segmentation of information
- Multi-factor authentication
- Develop incident response plan

3rd Party Experts

- Utilize consultants that specialize in high risk areas
- Shift liability to vendors
- 3rd party risk questionnaires
- Develop relationships before a crisis

Infrastructure Security

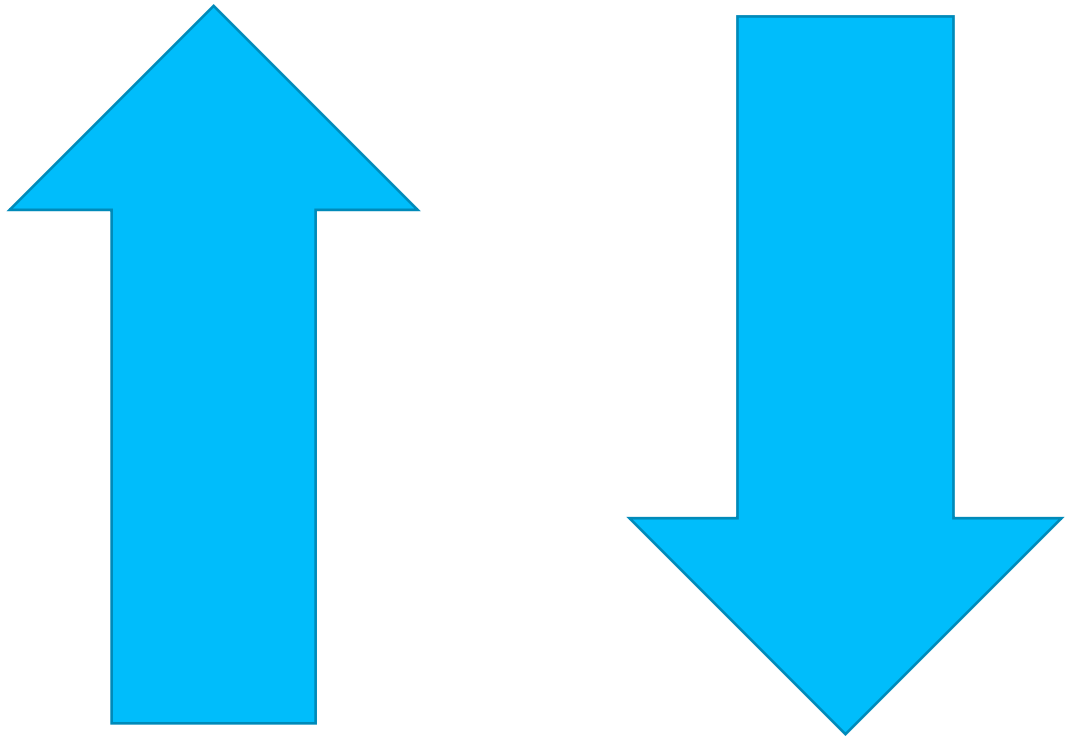
- Invest in up to date hardware and software
- Perform regular updates
- Patch management
- Cloud-based platforms
- Data back up solutions

SECURITY

INVESTMENT

TRAINING TIME

TRANSPARENCY



CONVENIENCE

BUDGETING

PRODUCTIVITY

IMAGE

THANK YOU