THE ULTIMATE CYBERSECURITY RESPONSE GUIDE for Gulf Coast Municipalities to Prevent Interruption of Government Operations

Learn how to reduce the risk of a public ransomware attack and minimize the impact upon breach

Business Information Solutions, Inc. | www.askbis.com | Phone: 251.410.7601

UNDERSTANDING THE RISK OF A CYBER ATTACK

Every week, there's an article about another U.S. city falling victim to a cyber attack. Just by the sheer number of breaches, it's clear that hackers have set their sights on infiltrating government entities and aren't going to stop any time soon.

According to The Wall Street Journal, the top 25 cities in America have already purchased cyber insurance or are in the process of looking into it. They have finally come to the conclusion that cyber threats are only growing stronger and more complex by the year; so, it's time to protect themselves. One weak link in the system starts off a chain reaction. Since systems within the government are interconnected, it leads to one network compromising the other. The only way to minimize the impact is to have a comprehensive cybersecurity response policy in place.

Why Do Hackers Target Municipal Governments?

Interconnected Systems & Internet of Things

Vulnerabilities Due to Size & Structure

Gold Mine of Sensitive Information

Financial Budget Constraints on Cybersecurity

Government Cybersecurity Stats

97%

do not have an effective disaster recovery plan

Pivot Point Security Survey

46%

do not store their files offsite

Pivot Point Security Survey

90%

do not encrypt emails with sensitive information

Pivot Point Security Survey

78% of Cities & Towns Do Not Have an Adequate Policy in Place for Managing Passwords

Pivot Point Security Survey

The CISO of Los Angeles said governments should be allocating 15% of their budget to cybersecurity

Data-Smart City Solutions

60% of people are not aware of the security risks at their organization

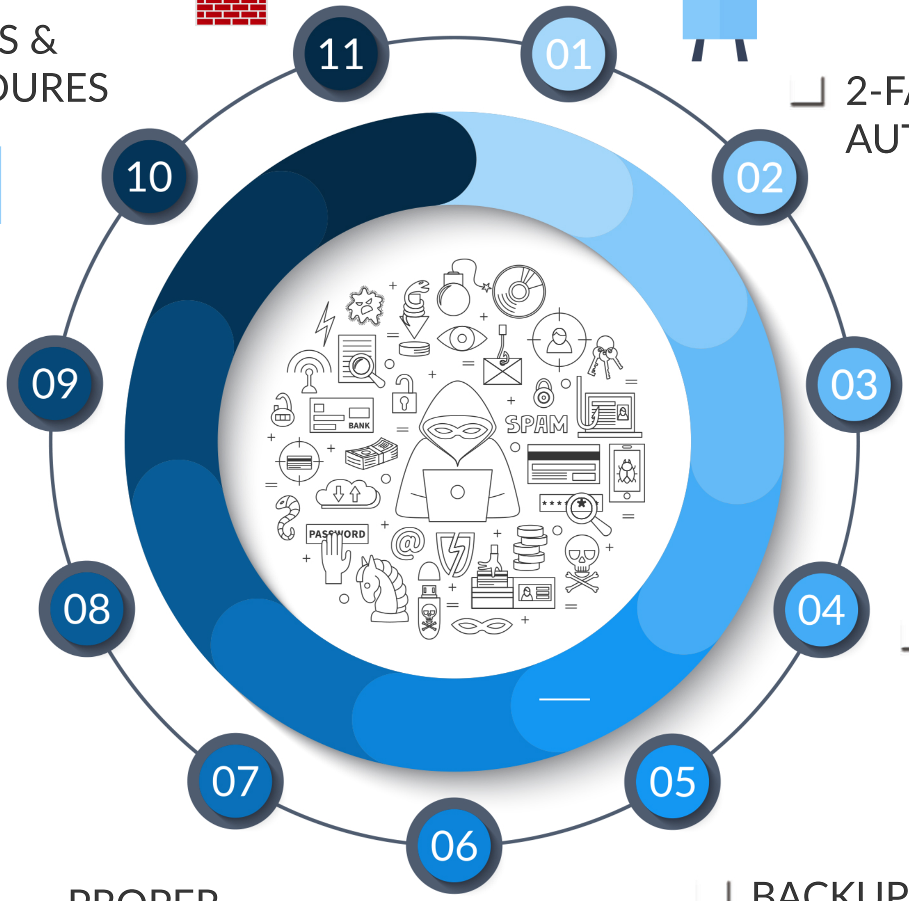
Ponemon Institute Survey

bis

Getting IT done.

11-STEP DEFENSE-IN-DEPTH STRATEGY TO PROTECT AGAINST RANSOMWARE

The best defense against cyber threats is a strong offense. Municipalities should proactively implement the following security protections to stay one-step ahead of hackers.



□ SECURITY AWARENESS TRAINING

□ 2-FACTOR AUTHENTICATION

□ PATCHING

□ EMAIL FILTERING

□ BACKUPS

□ RISK ASSESSMENT

□ PROPER CONTROLS

□ SECURE VPN

□ DISASTER RECOVERY PLAN

□ POLICIES & PROCEDURES

□ ANTI-VIRUS & FIREWALL

CYBERSECURITY INCIDENT RESPONSE POLICY

22% of breaches took more than a month to contain, remediate & recover

The only way to minimize the impact of a security incident or breach is to be prepared. With a comprehensive cybersecurity response policy, you'll have everything you need when a security incident occurs. This is especially helpful if systems are down and you cannot access this information.

However, it's not enough to just have the policy, you must train your staff on it in order for it to be successful. Otherwise, you'll have a great plan that nobody will know how to implement.

Your Incident Response Policy Should Include:

- Threat assessment center
- Incident management team
- Damage assessment team
- Disaster recovery plan with offsite backup
- Incident response plan with probable plan scenarios
- Documented alternative work sites
- Defined recovery objectives
- Notification plan with various statements for public
- Notification plan with various statements for internal
- Vendor and business associates list with contacts
- Systems restoration plan according to priority
- Cyber liability insurance policy with contacts
- Qualifications for putting the response plan into action

https://www.masc.sc/SiteCollectionDocuments/Internet-Technology/AM-15Protecting%20City%20Data.pdf

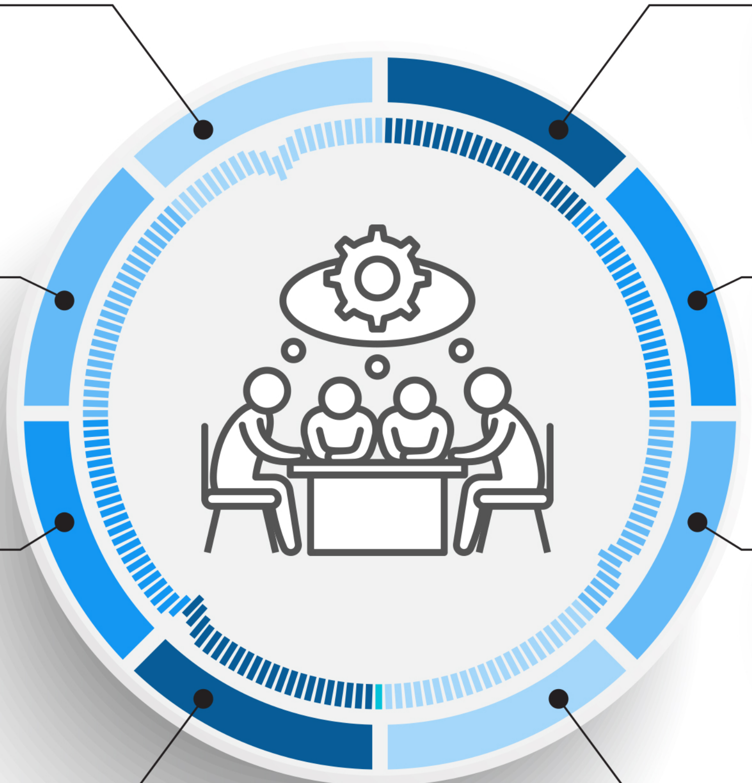
WHAT TO DO ONCE YOU'VE BEEN BREACHED

bis
BUSINESS INFORMATION SOLUTIONS

Getting IT done.

Even after you've implemented the proper security protections, there's still a chance of getting breached. Luckily, your comprehensive, cybersecurity response policy should minimize the impact and keep interruptions of government operations to a minimum.

Here are the steps you should immediately take upon learning of a security incident or breach:



Step 1
Assemble your incident response team

Step 2
Notify your IT department immediately

Step 3
Identify the cause & isolate the infection

Step 4
Communicate with the entire organization

Step 5
Reach out to your cyber insurance provider

Step 6
Investigate & remediate the issue

Step 7
Issue a statement to the public

Step 8
Report the incident to federal & local authorities

You can report a cybersecurity incident to the Department of Homeland Security by visiting: https://www.us-cert.gov/forms/report

bis BUSINESS INFORMATION SOLUTIONS Getting IT done.

DON'T LET HACKERS WIN!

Every 40 seconds, an organization is hit with ransomware!

My name is Phillip Long and I'm the CEO of Business Information Solutions. As a cybersecurity specialist, I continue to see cities and towns who are blindsided by cyber attacks that shut down government operations and cost them thousands of dollars to recover data.

It's my duty to warn as many municipalities as possible against the real threats they face so that they can protect everything they have worked so hard to build. Even if you've already got a guy, it's extremely important to get a second opinion because you don't want to wait until it's too late!

Phillip Long, CEO & CISSP

{FREE} CYBERSECURITY TRAINING WORKSHOP

Here's what I'm going to cover:

The latest active cyber threats

How to spot a phishing email

Defense-in-depth strategy

This offer includes:

- ✓ 2-hour, onsite training workshop
- ✓ Cybersecurity workbook for your staff
- ✓ Network evaluation
- ✓ One-page technology roadmap
- ✓ Dark web scan with report
- ✓ Copy of my book

Call 251-410-7601, email security@askbis.com or visit www.askbis.com/government-workshop to redeem this offer!