DYNAMIC SYSTEMS INC.®

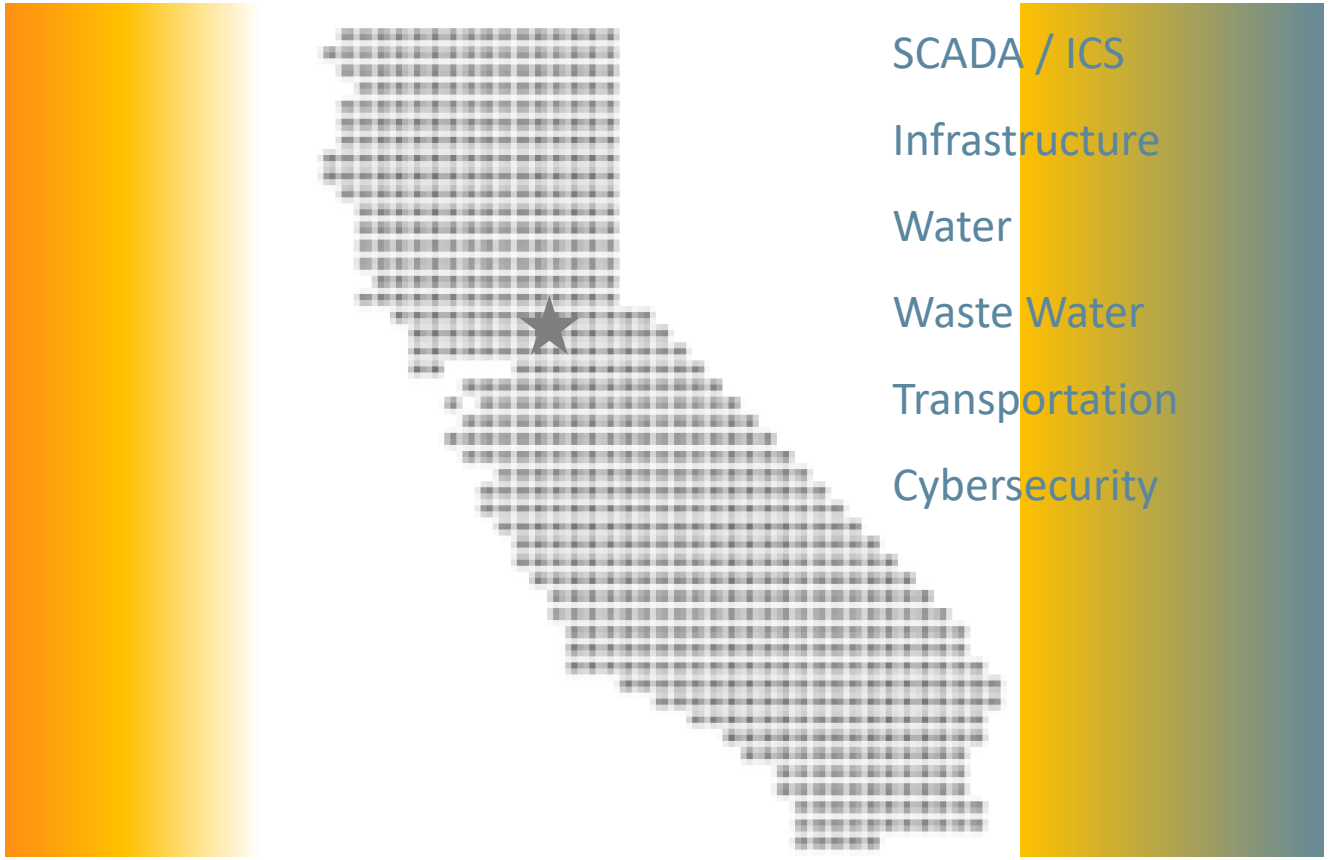
Your Data is Our Business

# Are You Cybersecurity Ready?

mike.williams@dynamicsystemsinc.com

# Critical Infrastructure Security Forum 2019

- ✓ Cyber Preparedness
- ✓ Lets Play 20 Questions
  (Based on the book “Secure Enough” by Bryce Austin)
- ✓ How Can We Help?
- ✓ Resources



# Question #1

## Why is Cybersecurity a problem for my company?

What is our liability if a cybersecurity incident causes a production outage or a data exposure?

What regulatory concerns do we have if a breach occurs?

# Question #2

DYNAMIC SYSTEMS INC.®

## Where is my data, and how can I keep it secure?

What sensitive data does your department create, consume, and store?

What protections exist to keep that data secure?

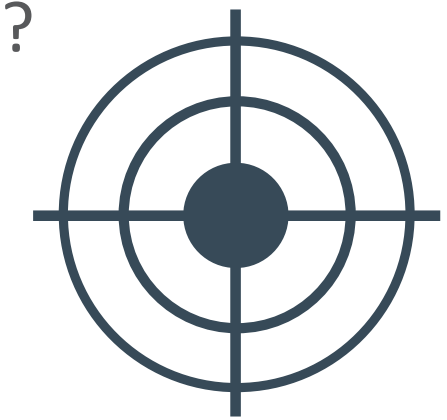
Who determines where your department's data sits, both inside the company and outside?

Who determines who gets access to which data?

# Question #3

**How valuable a target is my company to cyber criminals?**

Who in our industry has been hit by cybersecurity incidents?



What commodity data do we possess that is valuable on the black market?

What is the total value of our data if it were to hit the dark web?

How much would we be willing to pay if someone was to shut down our business with a cyber-attack?

# Question #4

## Who are those potential cyber criminals?

Is our organization a target for Nation State level attacks?

Are we part of critical infrastructure, are we known as a leader in our industry, or are we in a type of business that other countries may object to?

Do we do business in a country where we may be caught in the crossfire of Nation State attacks?

# Question #5

## Why isn’t law enforcement doing more about cybercrime?

Do we have Federal and local representatives for cybercrime prevention?

What is our policy on when we reach out to those agencies?

Who has the authority to make that decision?

# Question #6

## Who is responsible for cybersecurity concerns at my company?

Do we have a policy on who can proactively shut down systems based on a concern of cybersecurity risk?

Who is the decision maker if an incident is a cybersecurity issue?

# Question #7

**What is the first call I should make if my team suspects a breach?**

Do we have a playbook on how we investigate suspected cybersecurity incidents?

What is our communication and escalation process on suspected incidents?

# Question #8

## What do my employees need to know about cybersecurity?

When was the last time you were trained on cybersecurity?

Do your team members who have access to sensitive data get additional training above and beyond those who do not?

What did you take away from it?

# Question #9

**What standards or regulations for cybersecurity should my company use as the basis for a cybersecurity program?**

- What regulations is … llow due to our industry?
- What regulations is … llow due to our geography?
- What cybersecurity … seful for our business?
- Where are we on im… maturity of the framework(s) we choose to follow?

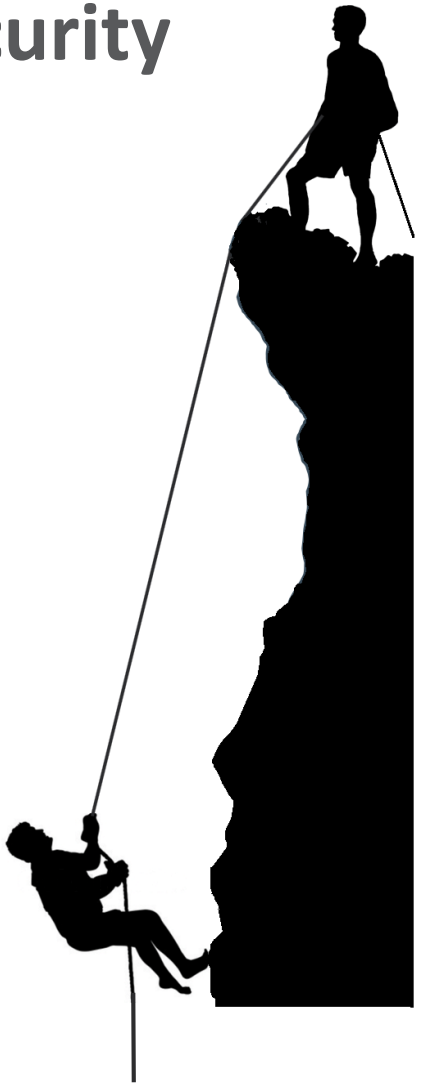
# Question #10

**How much would my customers care about a cybersecurity breach?**

How important is customer trust to our brand?

Do our competitors try to differentiate themselves based on trust?

What is it that we must protect to maintain our customers' trust?



# Question #11

## What is my playbook if I have a cybersecurity incident?

How do we test our incident response playbook?

How often do we test it?

What did we learn from our last test?

# Question #12

DYNAMIC SYSTEMS INC.®

## Will my incident-response plan work the way it should?

How does our company assess the success/failure of an incident response test?

When was the last time a test was done and what were the findings?

Which systems would shut down our business if we lost them?

Has our incident response plan ever been run by someone outside of the technology team to ensure that the leader in this department isn't the only person that can execute it?

# Question #13

**What are all these “Next-generation Firewalls”, “Intrusion Prevention Systems”, and “Security as a Service” systems that people are trying to sell my company?**

Do we have the right tools to detect cyberattacks?

Do we have the right tools and vendor partners to react to a cyberattack?

Do we have the right tools to protect against cyberattacks?

Do we have trusted partners to help us make the decisions on the best tools?

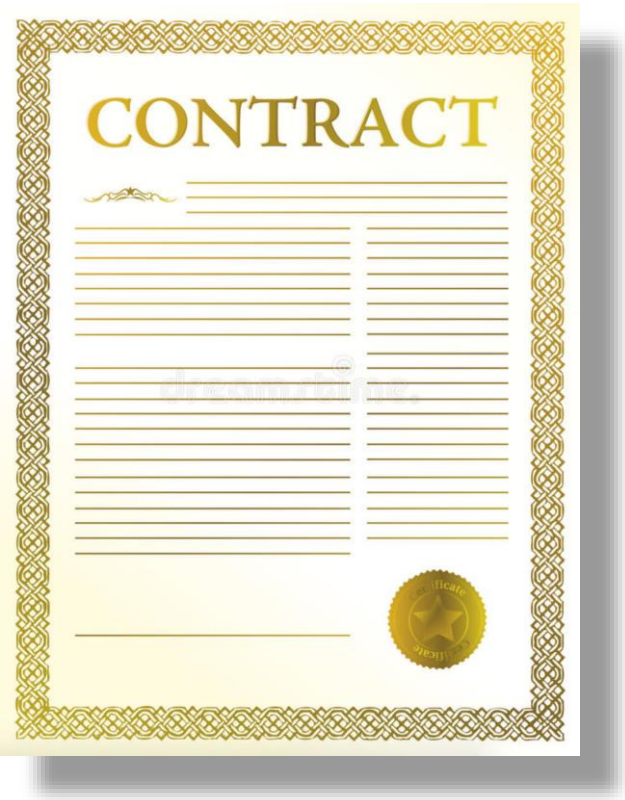
# Question #14

## Do our vendors care if they cause a breach of our data?

Do our contracts have language on cybersecurity?

What penalties or liabilities do we ask from our vendors in our contracts?

Which of our vendors have access to our sensitive data, and how do those vendor contracts differ from others?



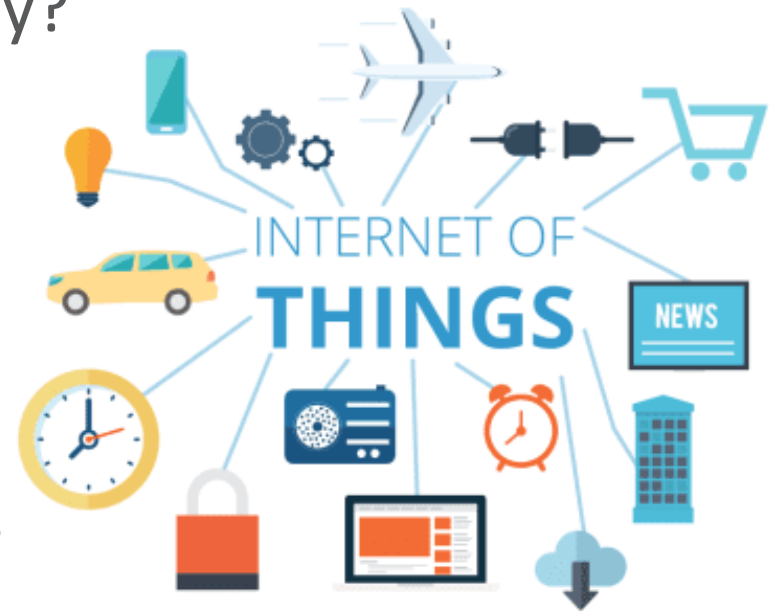
# Question #15

## What's all this "Internet of Things" stuff I have been hearing about?

What IoT devices exist within our company and why?

How many total devices are attached to our networks?

How do we know that the devices on our networks have a reasonable level of cybersecurity?



# Question #16

DYNAMIC SYSTEMS INC.®

## Are there things that I could be doing today around cybersecurity?

Are our systems all patched on a very regular basis?

Do we enforce password policies for every account in our company?

What is our cybersecurity awareness training program and why?

Do we use encryption for sensitive data and on all portable devices?

Do we review our list of who has access to what data, why, and how often?

# Question #17

## How can I keep myself educated on cybersecurity issues?

Do I have trusted sources for cybersecurity issues that impact my company?

Do I have a trusted advisory on cybersecurity issues?

What resources exist within my company that I could be leveraging to keep me informed on cybersecurity?

What cybersecurity events I should be participating in?

# Question #18

**Now that I know what questions to ask about cybersecurity, how do I keep these questions top of mind for my executive team, and my company as a whole?**

Are my management reviews inclusive of cybersecurity concerns?

Do I challenge my team to address cybersecurity for their departments?

What company events do we have where cybersecurity could be a theme, or at least a topic of discussion?

# Question #19

## Where is cybersecurity headed?

Which cybersecurity trend is the most concerning to our company?

Which cybersecurity trend is the most concerning to our industry?

What are we doing to respond to that trend?

# Question #20

## How can cybersecurity be a competitive advantage for my company?

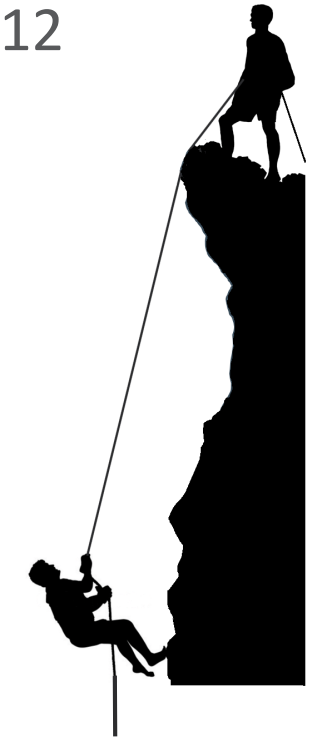
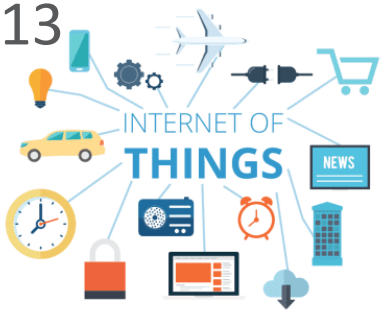
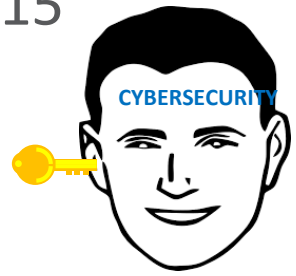
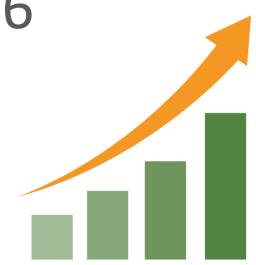
Is cybersecurity becoming a competitive differentiator in our industry?

Could it be a differentiator for us?

What are we doing to embrace cybersecurity as a means to bring competitive advantage?

# Summary Chart

DYNAMIC SYSTEMS INC.®

| | | | | | |
|---|---|---|---|---|---|
| 1  | 2  | 3  | 4  | 5  | 6   |
| 7  | 8   | 9   | 10   | 11   | 12  |
| 13   | 14  | 15   | 16  | 17  | |

# Summary Chart (cont.)

18. How will you know your plan will work?
19. What devices do you need to Detect, React, and Protect against cyber breaches?
20. What can you be doing today about Cybersecurity?

# What Can We Do to Help?

- Dynamic Systems, Inc. - small, woman-owned systems integrator and reseller (1991).
- Professional Services - deep bench of experienced system architects & engineers.
- Maintain a large pool of TS/SCI cleared personnel.
- Specialize in system security design and implementation.
- Many engagements with DOD, DOE and others on system hardening and security.
- Always deal from a position of integrity.
- We are considered a trusted partner with our customers.
- We are not in business to own customer systems or prolong engagements.
- We are in the business of planning and facilitating customer success.

# Resources

- Dynamic Systems Inc.
  - https://www.dynamicsystemsinc.com
- “Secure Enough”
  - By Bryce Austin ISBN: 978-0-9993931-0-9
- Account Executive Contact:
  - Ken Clement <ken.clement@dynamicsystemsinc.com>
  - (916) 872-3521