



IGFOA ANNUAL CONFERENCE

Moving into the Future with Purpose

Springfield, Illinois
September 9-11, 2024

Navigating
Cybersecurity: Master
the Controllable;
Brace for the
Uncontrollable

September 11, 2024

Agenda

- Cybersecurity in 2024
- Why Government?
- Most likely threats
- What is in your control, and what is not
- Bracing for the uncontrollable
- Questions

Introduction



Natalie Schwarz

Principal

Information Technology Consulting Public Sector



In our 100 years in business, we've grown to be one of the nation's largest audit, tax, consulting, and wealth management firms. Our more than 3,500 professionals, with experience working in over 150 countries, are committed to exemplary client service every day and everywhere.



“What would you say you do here?”

Where you think you are

Where you are actually

Where you need to be

Organizational
blind spots

Know control
weaknesses

Actual controls
in place

Additional control
opportunities

The plan forward

Cyber Security in 2024

What Should CFO's Know

- Technologies: constantly advancing
- Hackers: stronger than ever
- Reasons: ever expanding
- Business Perception: Security = IT
- Problem: resources (supply) < demand
- People: have day jobs unless security is primary
- Incidents: not if, but when
- Cost of a Breach: rising (dramatically)
- Citizens: expect security



Why Government?

The Stakes are High

Staffing gaps

- Government agencies often have limited staffing resources

The value of sensitive data

- Governments store vast amounts of data (e.g. citizens personal data)

Political or economic impact

- Hackers may aim to influence political decisions or disrupt essential services

Aging technology

- Makes governments vulnerable

Limited budget for security

- Makes governments even more vulnerable



Most Likely Threats from Hackers



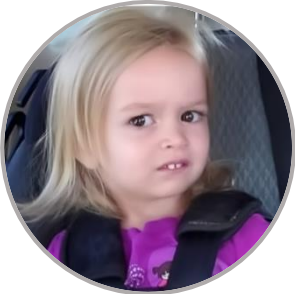
Ransomware

- Disruption of service
- Citizen harm
- Financial loss



Data Theft

- Regulatory fines
- Legal repercussions
- Loss of citizen trust



Supply Chain Vulnerabilities

- Data theft (above)
- Disruption of service
- Potential financial loss

How will they get you?



Phishing



Phone



Physical Access

“Expect phishing attacks to continue to rise”

- Captain Obvious



You have to have seen this one coming?

I Spoke with my IT
Guy, he told me:
“don’t worry, we’re
safe!”

Many of the vulnerabilities exploited through 2024
continue to be ones known by IT professionals at the time
of the incident

But it's not just about technical vulnerability



The refurbished printer.



ADP in the cloud is easier for everyone, if you let it!



Email is the control, but is that a good thing?



It's time to make a **CHANGE**

Let's talk about Change

Months later, details of Alaska cyberattacks remain a closely held secret

The Tyler Technology Ransomware Attack

At the end of September 2020, the company disclosed the fact that it suffered a ransomware attack with its customers apparently finding suspicious logins and previously unseen remote access tools on their networks

Troup: Quincy facing one of the 'worst cyber attacks' to ever hit the community

U.S.

Cyberattacks on water systems are increasing, EPA warns, urging utilities to take immediate action



What did Executive Learn from Change?

Although cost effective, maybe it isn't a good idea to rely on a single provider for so many critical business processes?



What did Executives Learn from CrowdStrike?

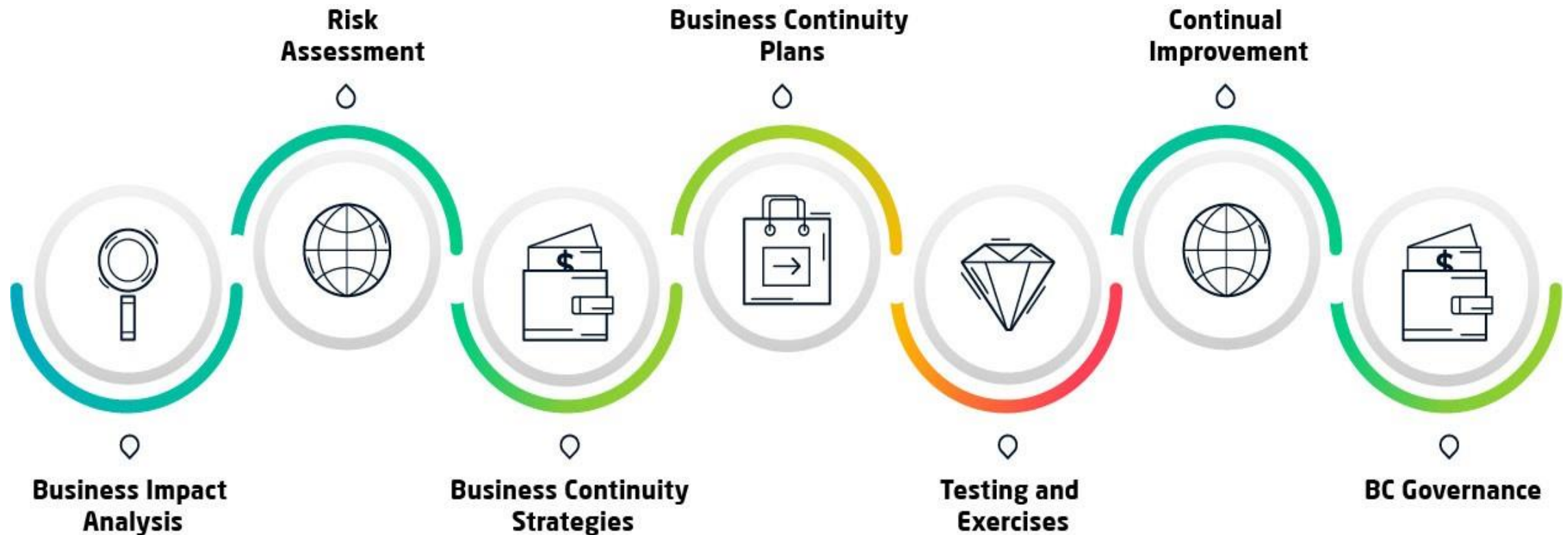
Maybe Business Resilience is the responsibility of every department? And hopefully each department has continuity plans for continuing business manually~

And they all lived happily ever after~

~The end

Are you ready to Change?

Based on what you've learned this year, where should you be involved?



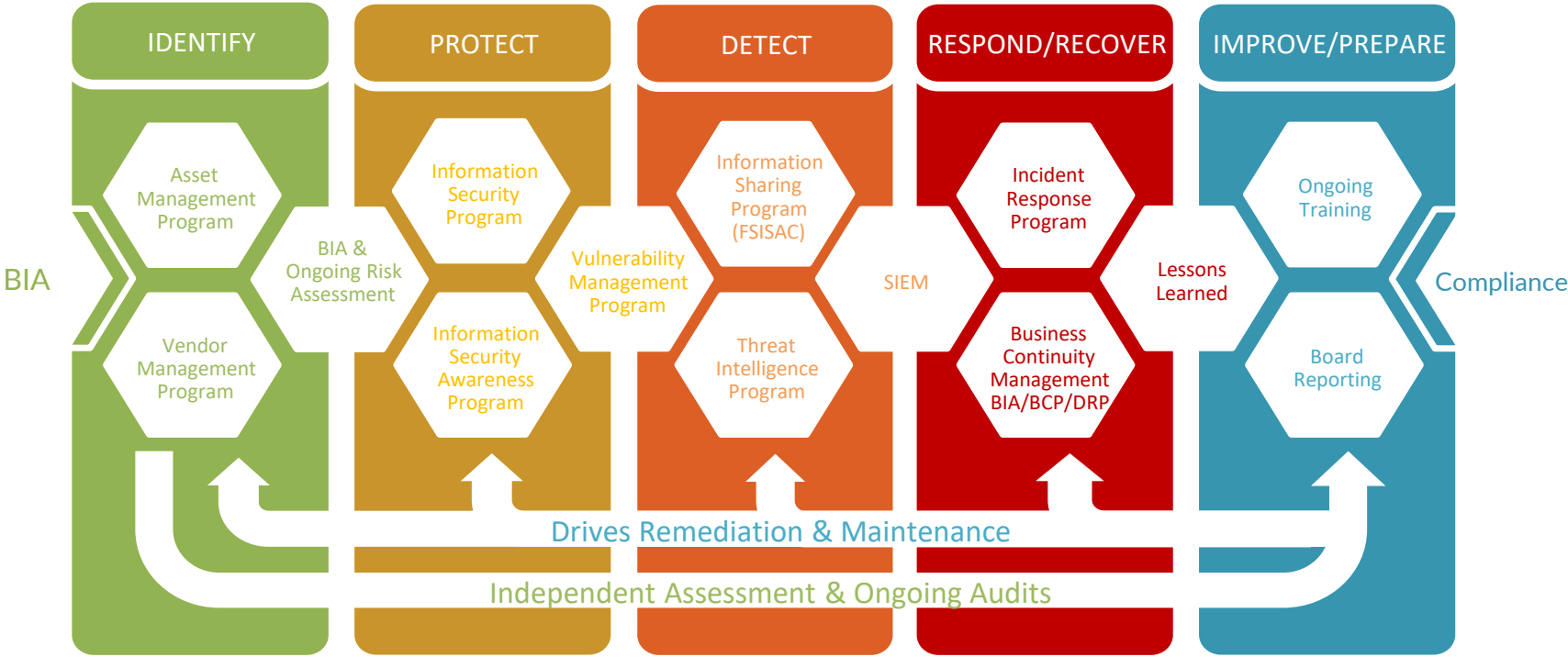
Is all hope lost?

“The secret to your future is hidden in your daily routine.”



A roadmap to limiting risk

“The controls you’ve implemented today won’t necessarily address the risks of tomorrow.”



Final Thoughts....



Assess environment for security risks



Implement cyber security policies



Train staff on security awareness best practices

Natalie Schwarz

Principal

Information Technology Consulting
Public Sector

natalie.schwarz@plantemoran.com

