Under Pressure: Management, Compliance, and Cost of the Data/IT Enterprise

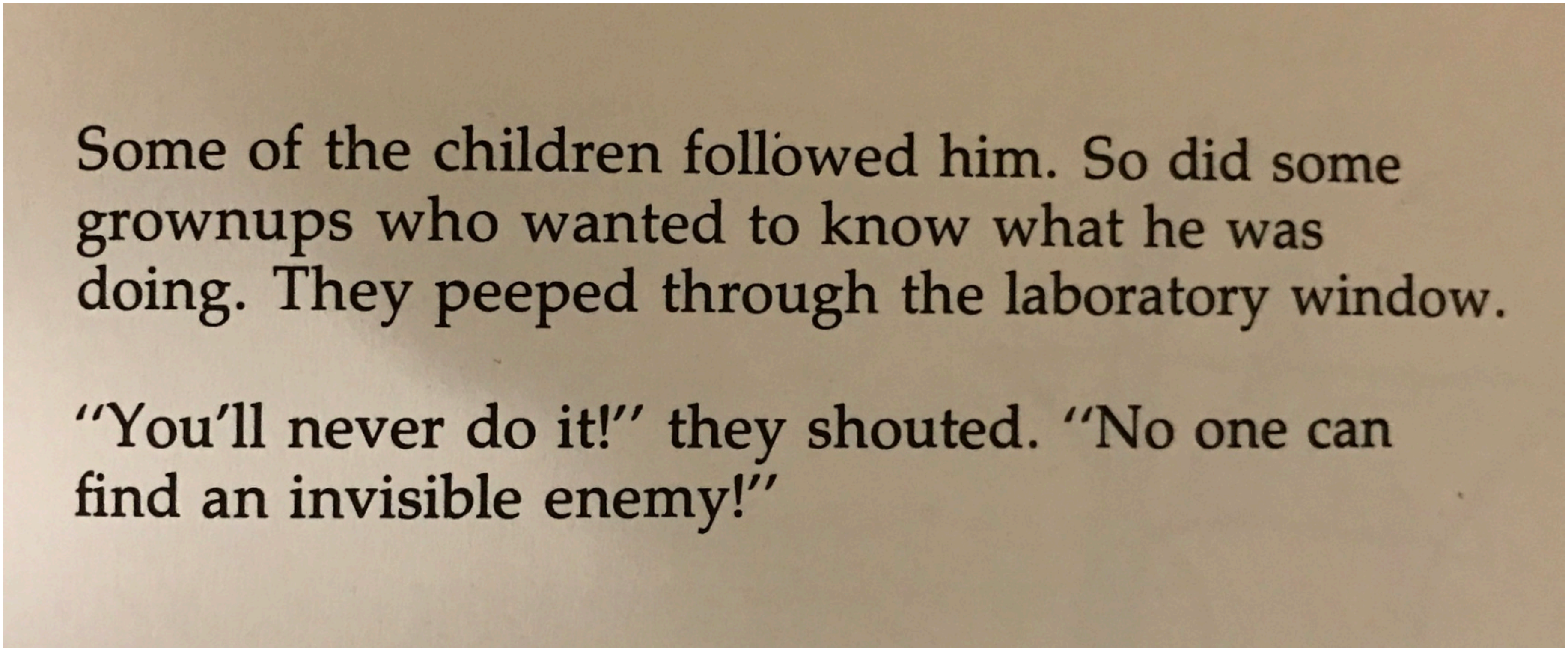
COGR Meeting – Washington D.C.

June 8, 2017

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

GW Division of Information Technology

About Me



Some of the children followed him. So did some grownups who wanted to know what he was doing. They peeped through the laboratory window.

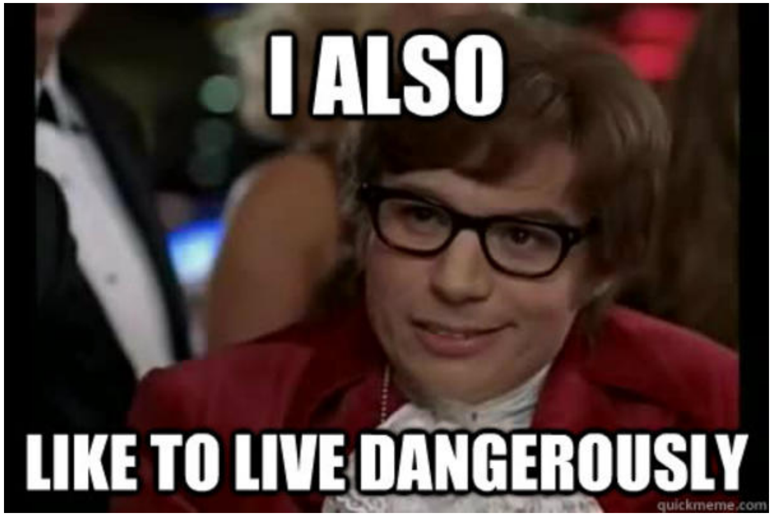
"You'll never do it!" they shouted. "No one can find an invisible enemy!"

Johnson, Spencer, and Steve Pileggi. *The value of believing in yourself: the story of Louis Pasteur*. La Jolla, CA: Value Communications, 1976. Print.

InfoSec in Higher Education - Challenges

- Colleges and universities are cities
- Varying degrees of data sensitivity from public to non-public to regulated
- Hardware and software of all types: up-to-date, legacy, patched, unpatched, institutionally owned, BYOD
- Compliance requirements (FERPA, HIPAA, PCI-DSS)
- Culture of openness and experimentation
- Compressed budgets and talent shortages to manage all of the above

- Focus on risk
- Build relationships and a culture of awareness
- Work with faculty, researchers, staff, and students
- Focus on process maturity
- Invest in people

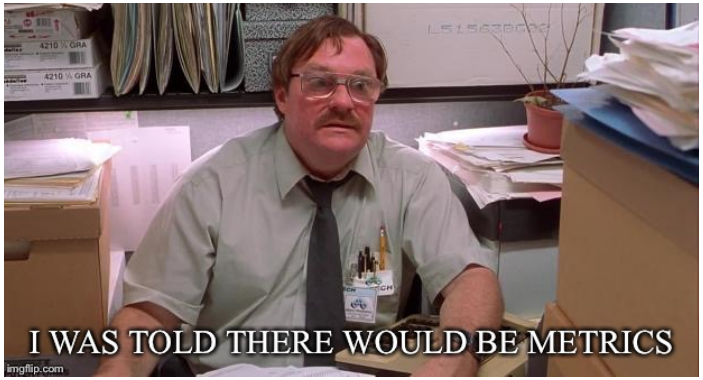


InfoSec in Higher Education – Meaningful Controls

- People > technology
  - Hire curious, talented people
  - Work with and train your users
- Border firewalls are your friend
- Good firewall rules and governance are your best friend
- Two-factor authentication
- Visibility, logging and analytics
- Patching and hardening
- Continuous monitoring

InfoSec in Higher Education – Building Support

- Working in compressed/challenging budget conditions:
  - Work with board, executive leadership
  - Establish a governance model
  - Understand the risk tolerance
  - Evaluate current spend, current scope
  - Evaluate and report risks
  - Tools are attractive but require staff to configure, manage, and utilize
  - Supplement staff if you have gaps
  - Report out on risk mitigation
  - Document everything



InfoSec in Higher Education – Research Considerations

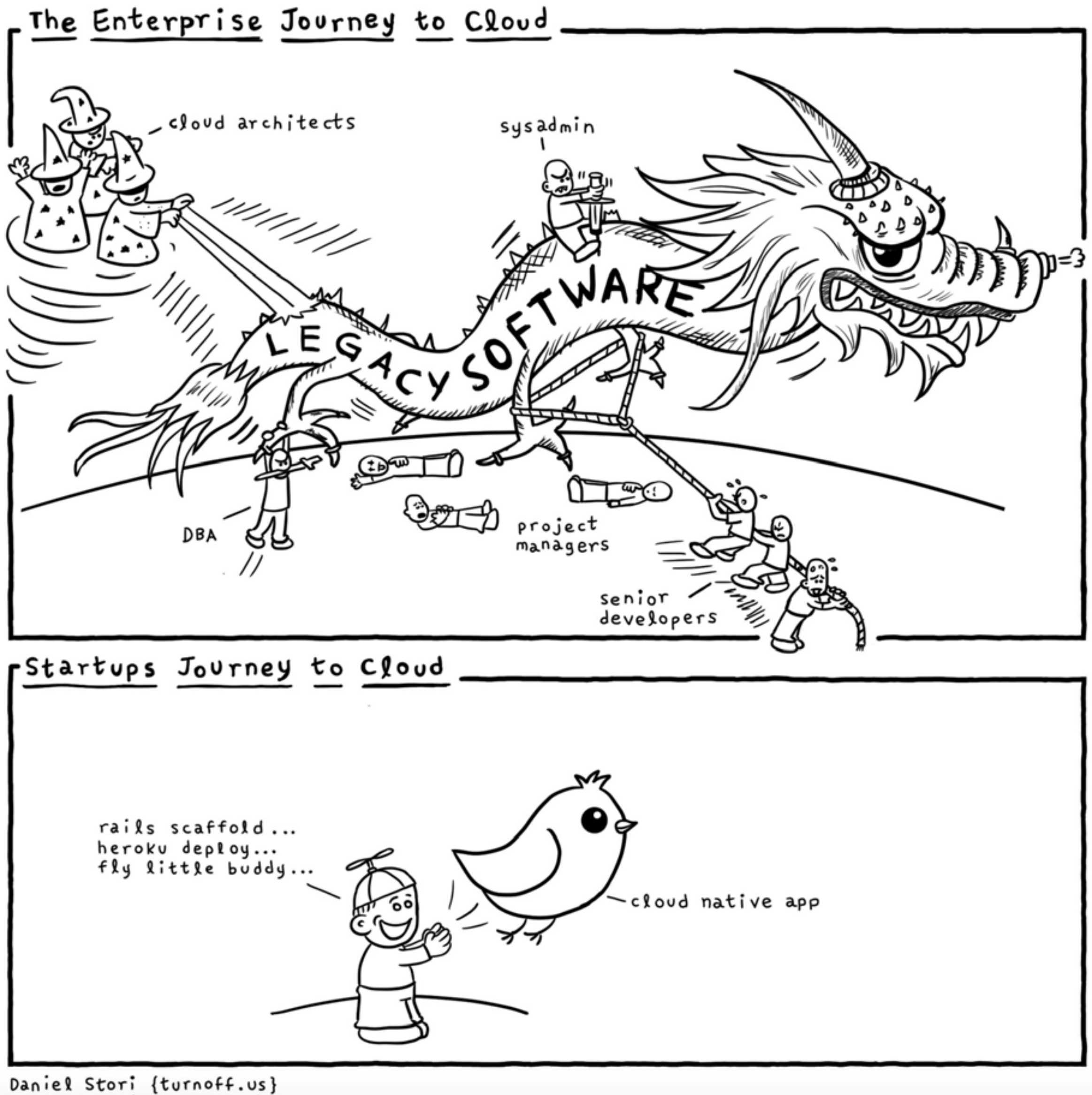
- Research compliance AND security
- Compliance != security
- Get involved early:
  - Review contracts and agreements
  - Review data management plans
- Work with researchers to develop scalable solutions
  - Process is king
  - Shared infrastructure
  - Common controls
  - Documented standards and good practices
- Start with NIST, NSF, and SURA

What keeps me up at night?

- Mishandling of non-public data
- Shadow systems
- What don't I know about?
- What can't I control?

COGR Meeting – June 8, 2017

What about cloud?

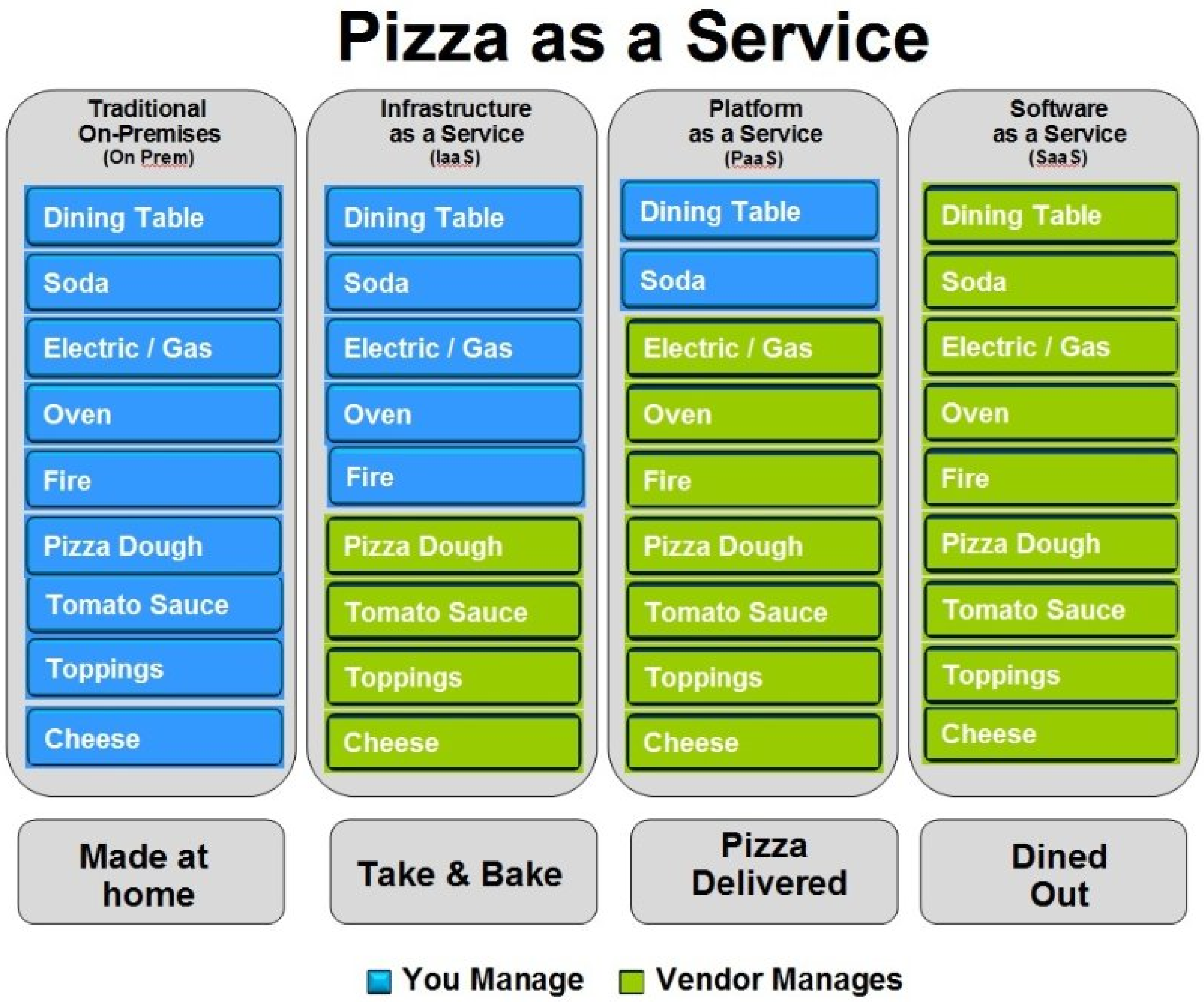


Daniel Stori {turnoff.us}
Thanks to Michael Tharrington

What about cloud? - Risk

- Not more risk, *different* risks
- Know what you’re getting and what you’re *not* getting
- Out-of-the-box compliance but…
  - Understand the “accreditation boundary”
  - What controls do you own?
  - You still have to do your homework

What about cloud? - Models



Pizza as a Service

Traditional On-Premises (On Prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough
🟦 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce
🟦 Toppings	🟩 Toppings	🟩 Toppings	🟩 Toppings
🟦 Cheese	🟩 Cheese	🟩 Cheese	🟩 Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

🟦 You Manage 🟩 Vendor Manages

What about cloud? - Assurance

- Review all assurance documentation:
  - SOC-2 (if you can), SOC-3 reports
  - Cloud Security Alliance
- Having a third-party or vendor risk assessment process is a plus

What about cloud? - Costs

- Cost transparency can be good but…
  - Internal IT can hide costs
  - Cloud can cost more than traditional on-premises compute/storage capabilities
- Billing
  - Defined services with defined costs
    - Make it easy on researchers; incentivize researchers to use these services
  - Lower the threshold to being secure
  - Not easy
    - Sometimes it’s easier to just buy a server than bill a grant for a service

COGR Meeting – June 8, 2017

In Conclusion

- Securing data in higher education is hard
- We can collectively do more to improve
  - Governance
  - Process
  - People
- Build a case for funding based on risk
- Compliance != Security
- Research data should be protected in a manner that meets compliance requirements and is reasonably secure (confidentiality, integrity, availability)
- Cloud *can* help, just know what you're getting into and how much it will cost