Kentucky Captive Association
2018 Educational Conference

Cybersecurity and the CEO

Thursday, December 13, 2017
with Robert Ramsay

BARNES DENNIG

Robert Ramsay leads the SOC Security practice at Barnes Dennig, a professional services firm in KY, OH & IN.

AICPA's Trust Information Integrity Task Force

"SOC Expert" with the AICPA

Peer reviewer for AICPA's SOC providers

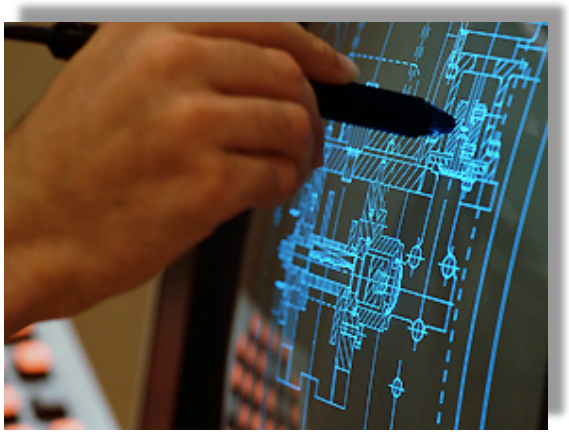
Formerly with PwC, Atlanta

HITRUST CCSFP, CISA, CITP, CPA

Indiana University, University of Louisville

Cybersecurity and the CEO

1. Big picture
2. Risk management
3. Staying current



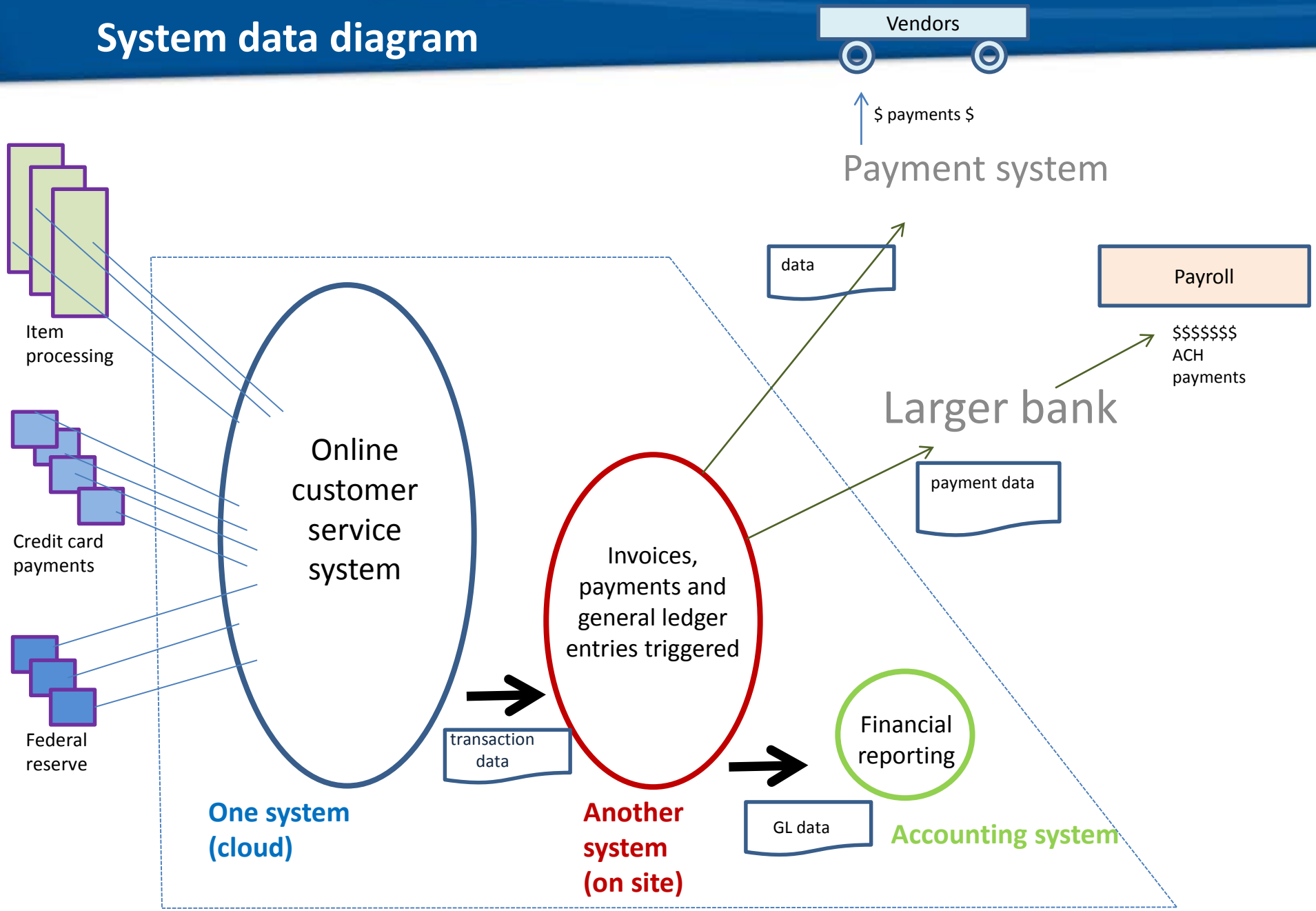
Advances in technology:

Robotics
https://www.youtube.com/watch?v=rVlhMGQgDkY

Artificial Intelligence
(True machine learning demonstrated)
https://www.youtube.com/watch?v=8fejJgHOGf0

Quantum Computing
https://www.youtube.com/watch?v=w_-_H9eBte8

System data diagram



Risk management

Cybersecurity frameworks or ISMS:

1. NIST Cybersecurity Framework
2. ISO 27001
3. HITRUST (HIPAA centric) Compliance framework
4. CSX Cybersecurity Fundamentals

Data security compliance requirements

I. Legal requirements
   A. HIPAA/HITECH
   B. GDPR
   C. KY HB 5

II. Contractual
   A. PCI
   B. SOC

Cloud-based software outsourcing – contract notes

Consider the following during contract negotiations with cloud-based software vendors

1. **Consider a breach notification clause requiring the vendor to notify you in the event the client recognizes a data breach.**

2. **Ensure the contract includes pricing for switching third-party vendors that impact the service.** (i.e. for a payroll vendor, what is the cost of changing the 401k provider or the health insurance TPA, if those services directly interact with the flow of payroll data).

3. **Ensure the contract includes procedures for obtaining your data in the event that the contract is terminated.**

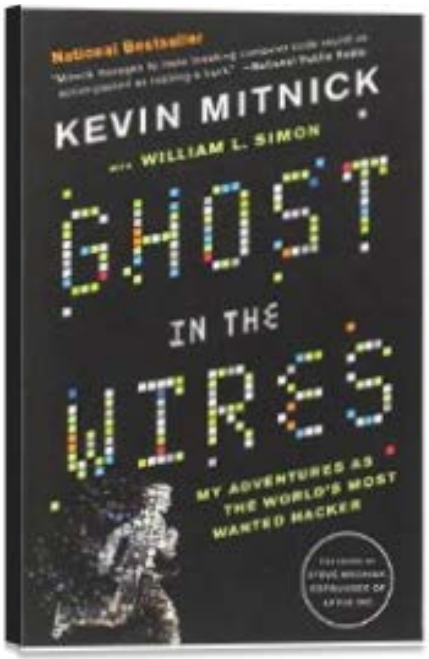
4. **Consider requiring the vendor to offer software in escrow.**
   This software would become the property of NAME in the event that the vendor discontinues the service or goes out of business. This is especially important for unique services that are difficult to replace. (i.e. this may not be as important for payroll since there are so many payroll providers)

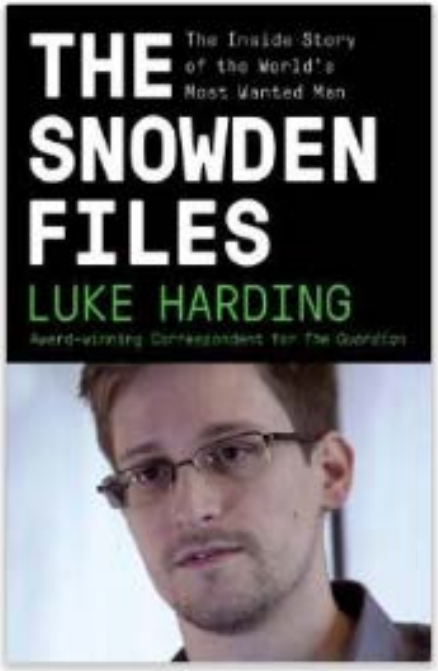
Buzzword update

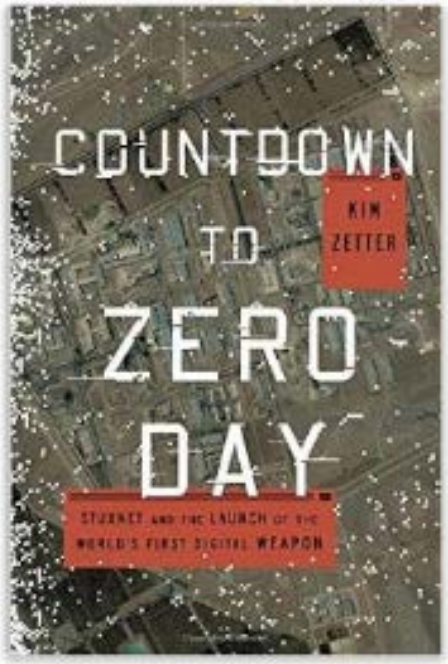
GDPR -
European Union's General Data Protection Regulation

Fileless malware –
Viruses that operate in RAM

Summer reading



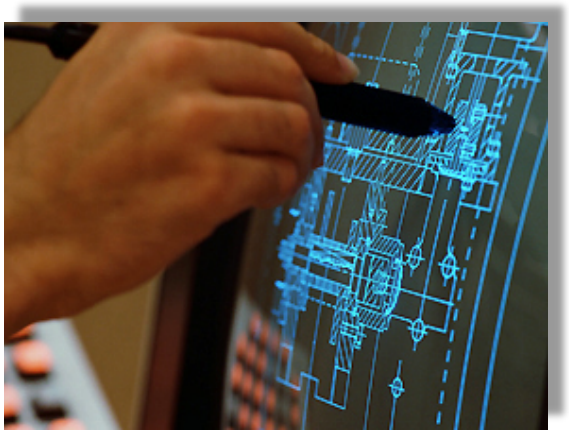




Ghost in the Wires, Kevin Mitnick
The Snowden Files, Luke Harding
Countdown to Zero Day, Kim Zetter

Cybersecurity and the CEO

1. Big picture
2. Risk management
3. Staying current



Questions / observations?

Robert Ramsay
513.929.6002
rramsay@BarnesDennig.com

Strategic Planning Spectrum