

2017 CIO Roundtable at ILTA

Thought Leadership in Action

August 13, 2017

Four Seasons Hotel - Las Vegas, Nevada



Security is not enough

Rethinking a Law Firm's Technology Strategy

Agenda

- Disruptive events in IT Legal
- The threat landscape
- Time for a Paradigm Shift?
- IT Strategy: An Alternative Approach
- Impact: Culture and IT
- Q&A

Preface

- Recent security attacks will impact how law firms look at their technology strategy
- Is the current infrastructure model good enough?
- Can law firms reasonably expect to secure systems to prevent massive business disruptions?
- What is the potential impact on firm culture and technology plans?

A Brief History of IT

Major Events in IT

The **Evolution** of the Datacenter

Many inventions over the past 70 years lead up to the modern datacenter. Let's take a look at some of the milestones that changed datacenter history.

stack*i*



1946

ENIAC (Electronic Numerical Integrator And Computer) was the first electronic general-purpose computer. It was digital and capable of being programmed to solve "a large class" of numerical problems.



1971

The Intel 4004 is a 4-bit central processing unit (CPU) released by Intel Corporation, and it was the first commercially available microprocessor.

SUNGARD

1978

Sungard Availability Systems became the first major U.S. commercial disaster recovery business.



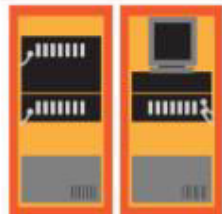
1981

The IBM Personal Computer, commonly known as the IBM PC, is the original version of the IBM PC compatible hardware platform.



Early 1990s

Microcomputers (now called "servers") started to find their places in the old computer rooms and were being called "datacenters".



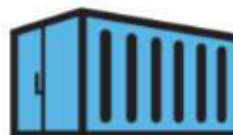
Mid 1990s

The boom of datacenters came during the dot-com bubble. Companies needed fast Internet connectivity and network operation to deploy systems and establish a presence on the Internet.



2002

Amazon Web Services begins development of a suite of cloud-based services, which included storage and computation.



2007

Sun Modular Datacenter is a portable datacenter built into a standard 20-foot shipping container manufactured and marketed by Sun Microsystems.



2013

Google invested \$7.35 billion in its Internet infrastructure. This spending was driven by an expansion of Google's global data center network. It represented the largest construction effort in the history of the datacenter.



2015

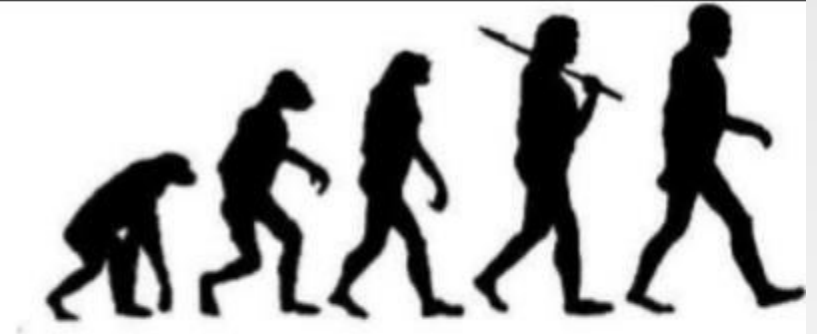
Over 5.75 million new servers are deployed every year. There are an estimated 4,500+ datacenters in the U.S. alone. To meet the growing demand of new applications and services, servers need to be deployed at an increasingly faster pace and larger number.

iPhone – June 2007



What about Cloud?

Evolutionary Path Forward



Disruption driven change

- The LAN/PC Age
 - Novell
 - WordPerfect
 - Lotus 1-2-3
- The Windows Age
 - Windows 3.1
- The Consumer Device Age
 - iPhone (2007)
- The Data Center age
 - Dot-com
 - 9/11
 - East coast blackouts

Malware: The Next Disruption?

The 'Wannacry' ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol

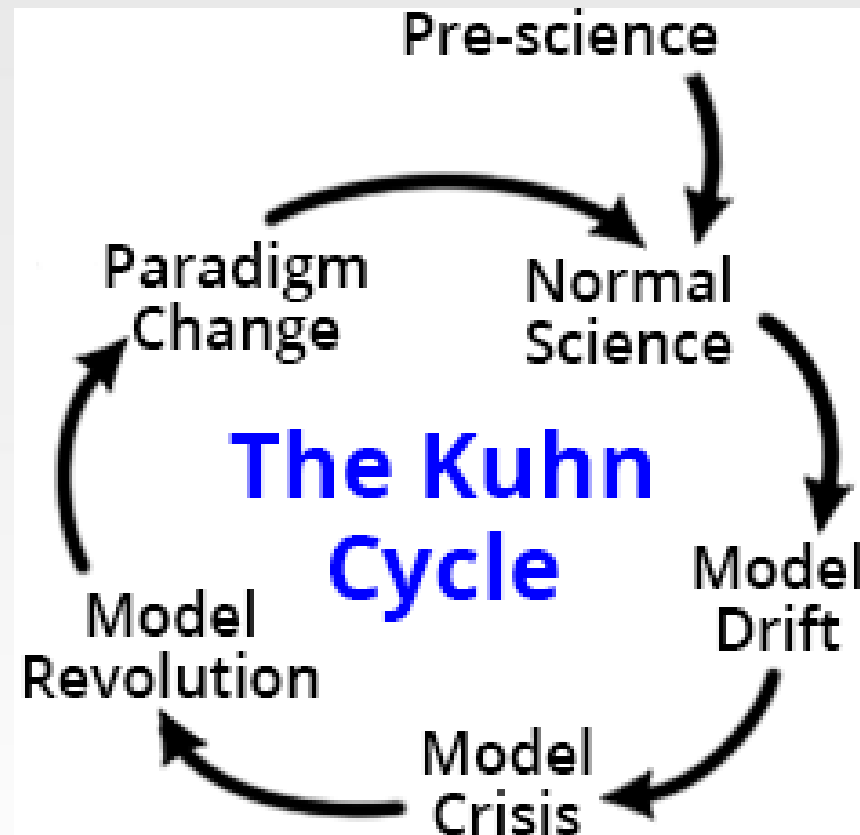


Source: Intel.malwaretech.com

© AFP

Time for a Paradigm Shift?

Detecting a Paradigm Shift



Normal Science – Build a Better Castle

- High availability
 - Dual-data center model
 - Redundant everything
- Encryption
 - Storage
 - End devices
 - Communications
- Perimeter defense
 - Firewalls
 - Intrusion Detection
 - 2-factor authentication



Normal Science – Build a Better Castle

- Allow access by Firm or personal devices
- Allow access inside and outside the Firm
- Replicate between data centers
- Assumes at least one combination of data center and user device will be available
- Highly successful model

Model Drift – Under Constant Attack

- Increased security spending
 - CISO
 - Security awareness training
 - Vendor assessments
- Usage Monitoring
- Cloud backup
- Threats well defined and managed
- Breach impact narrow and contained



How good are current models?

- Most assume breaches will be contained to specific areas
- Relatively easy to quarantine affected systems
- Recovery usually doesn't impact entire business
- In most cases correct:
 - Some workstations
 - Some storage locations
 - Some servers
 - One data center

So what is the problem?



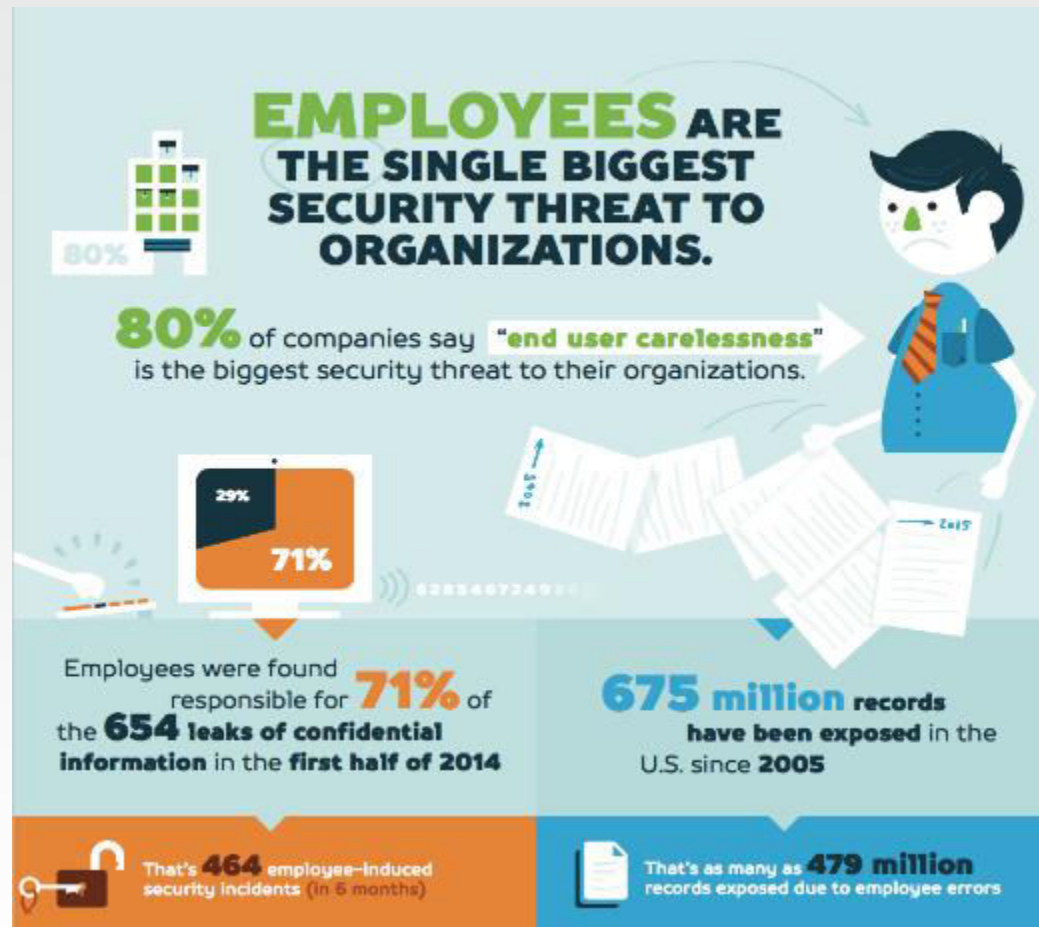
**Most models not really designed for
widespread/prolonged shutdown of
systems!**

Model Crisis – Bigger Threats

- More destructive
- More frequent
- Broader scope
- Longer impact
- What if you can't get to any of the data?



What is the real problem?



Is the Industry Prepared?

Logicforce Survey of 200 Firms

Law Firms Represented – by Size (number of attorneys)



Logicforce Survey

Every law firm assessed was
targeted for confidential client data
in 2016-2017

Approximately **40%** did not know
they were breached

66%

of law firms have reported a breach of some type, with varying levels of compromise.

80%

of firms are not vetting their third-party service provider's data security practices. Nearly 63% of breaches are linked to third-parties.

95%

of assessments done by LOGICFORCE show firms are not compliant with their data governance and cyber security policies. 100% of those firms are not compliant with their client's policy standards.

1 firm lost an entire practice group due to a failed audit.

18

law firms said they lost a client for failing an IT audit in 2016.

53%

of firms have NO data breach incident response plan developed.

60%

of firms do not have a specifically appointed Security & Compliance Manager and have no plans to appoint one.

88%

of AMLAW firms have cyber security practices.³

34%

of firms reported getting a client data security and systems audit in 2016. Based on industry data and survey responses, LOGICFORCE expects this to reach 50% in 2017 and 65% in 2018.

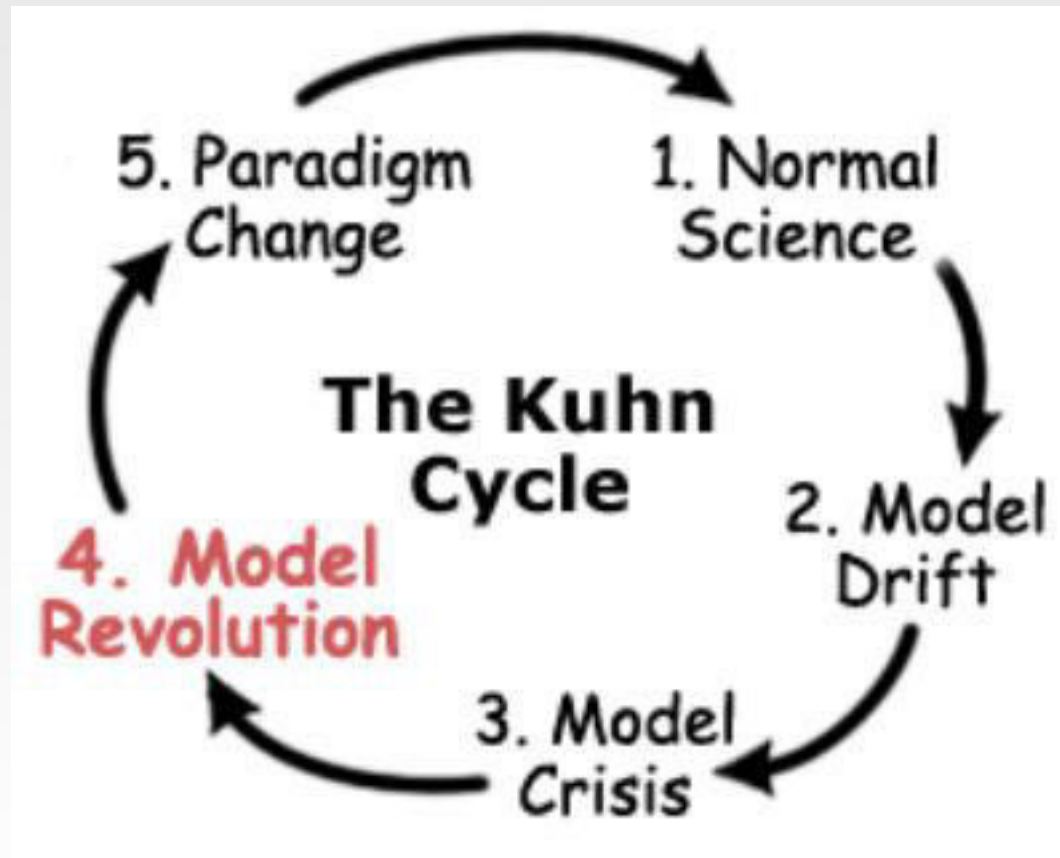
77%

of firms do not maintain any cyber insurance coverage.

Additional findings

- Only 25% of firms have full disk encryption across their entire organization
- 21% of firms have Multifactor Authentication
- 27% of firm have instituted DLP

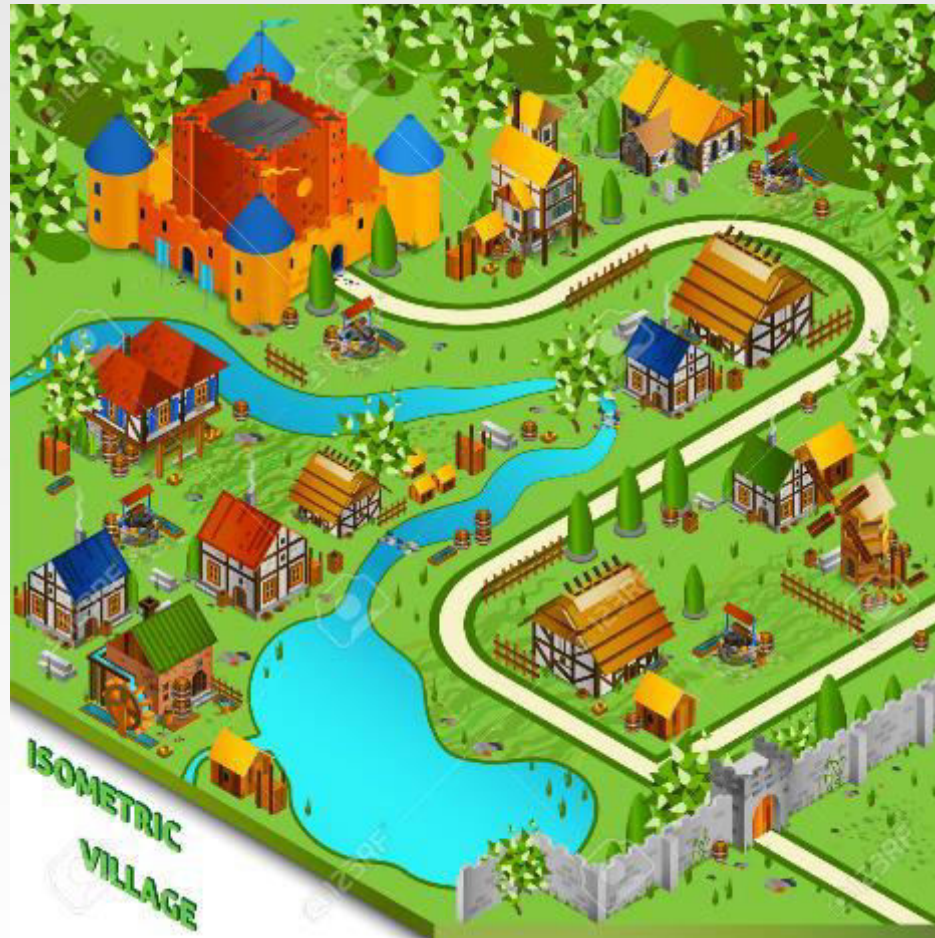
Is this really a Crisis?









Inherent Design Flaws?

- The private data center model
 - Everything under one roof
- Security is user-endpoint driven
 - Passwords
 - Physical device access
- The “Open” data model
 - People have access to the more than they really need
- Traditional desktops
 - Too personal
 - Hard to “wipe” reset in mass

Model Revolution – A Village not a Castle



Impact of a model change

 BUSINESS	 PLATFORM
 PEOPLE	 SECURITY
 GOVERNANCE	 OPERATIONS

Model Revolution – Rethinking IT Services

- Redefine role of IT
 - Protect IT and business operations
 - Major threat to business is real
- Make IG mandatory prerequisite to IT services
- Isolate users from data
- Security by obscurity
- Spread core systems beyond firm owned data centers
- Eliminate “personal” from computing

What are alternative models?

- Leverage multi-clouds
 - Spread core systems across platforms/vendors
 - The right vendors can enhance security
 - Harder to loose access to everything at once
- Adopt closed data models
 - Pessimistic DMS
 - Unstructured data management
 - Leverage tools to lock shares and force matter team access

What are alternative models?

- Identity Management
 - Make it hard to get to data
 - Associated access with the data, not the user
 - Must always validate your access
- Revise Incident Response Plans
 - Elevate risk of major disruptions
- VDI
 - Faster recovery of affected systems
 - Can “reset” all workstations in case of breach

**Is this really a paradigm
shift?**

Major Impact - Culture

- Will impose severe restrictions on how people store and access data
- Requires strong policies/Information Governance
- Identity based security is intrusive
- Can negatively impact workflow and collaboration
- Data owners must share security burden
- Major impact on KM

Major Impact – Budget & Operations

- Forces accelerated adoption of cloud
- Must develop comprehensive cloud strategy
- Must have solid vendor assessment programs
- More complex to manage
 - More vendors
 - Disperse systems
- Harder to provide “unified” user experience

Group Discussion – Are you ready?

- How does this new paradigm affect IT budgets?
- Does Firm management understand the risk?
- What happens when clients demand changes?
- Is your Incident Response Plan really ready for a widespread outage?

Questions and Discussion

