eSentio

CIO Roundtable

CIO Roundtable Atlanta
Rethinking BCP/DR

November 14, 2017

Agenda

- Welcome
- Upcoming Roundtable and Holiday Party, December 19th:
  - Holiday Party Following
- Host Introduction: Jamie Usher, Kilpatrick Townsend & Stockton LLP
- Today's Topic: Rethinking BCP/DR Strategies
- Participant's Expectations:
- Presentation/Discussion:

Presentation Agenda

- Threat's
- Rethinking the Data Center
- Preparedness
- Impact on IT
- Incident Response
- Summary

Today’s Threats

Today's IT Questions

- 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?

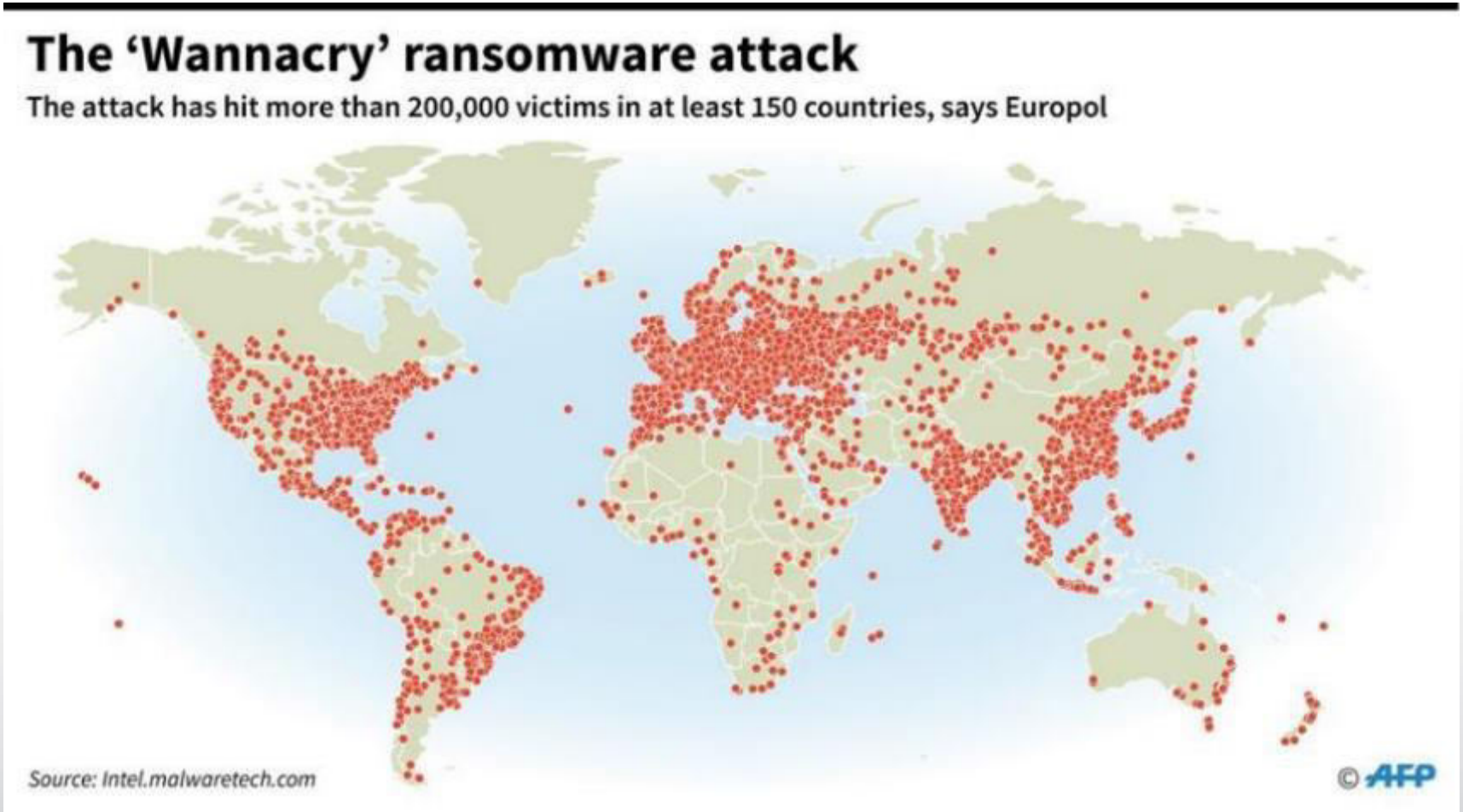
Recent Threats

- DLA Piper
- Panama Papers
- Wannacry
- Variants
- Cryptolocker

Ransomware

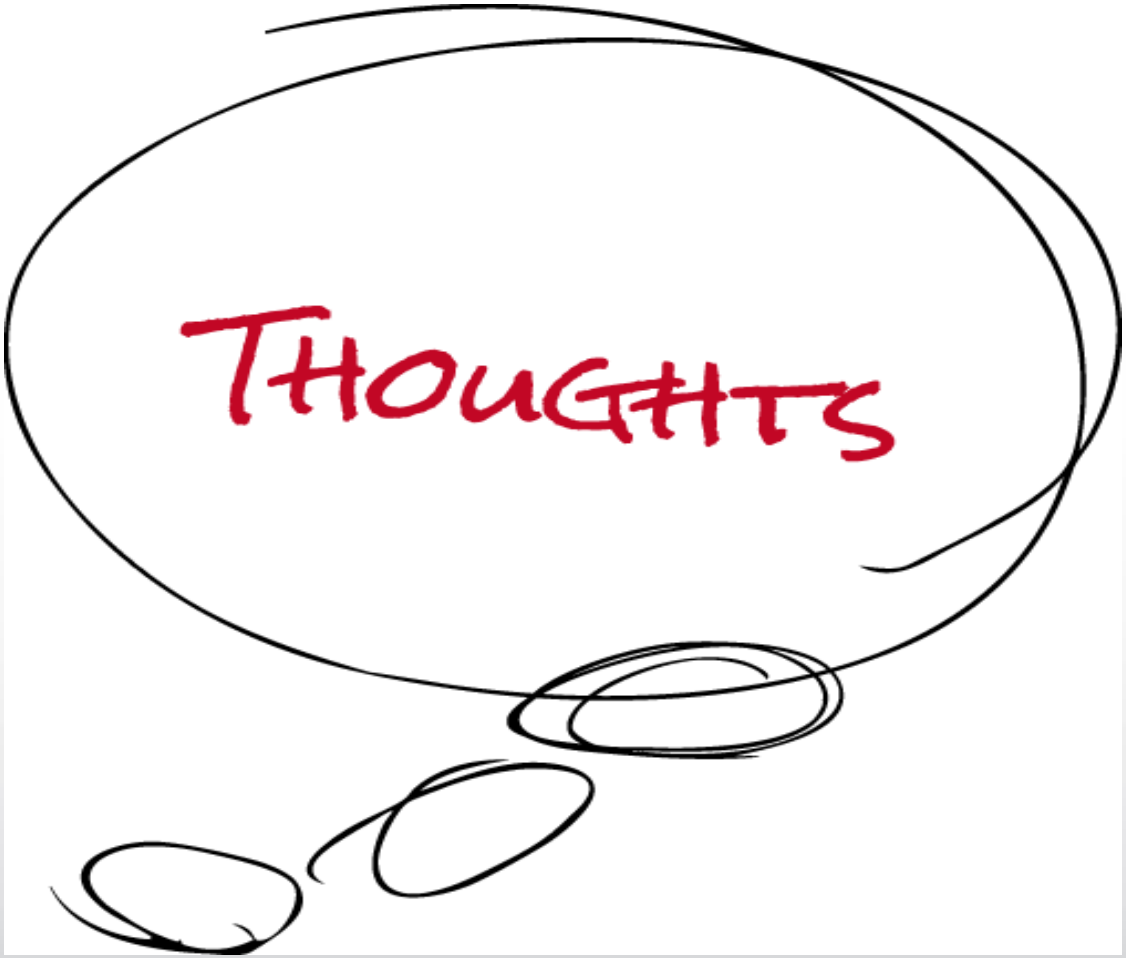

Wanna Decryptor 1.0
Ooops, your files have been encrypted!
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
How Do I Pay?
Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28
Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28
About bitcoin
How to buy bitcoins?
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
QR Code
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1
Copy

Today's Threats



How do they spread?

- Deceitful Website Downloads
- Malicious Email Attachment
- SPAM Software, Apps and add-ons
- Pre-existing infection
- Exploits and Vulnerabilities


THOUGHTS

Rethinking the Data Center

Incident Assumptions

- 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

Preparedness Assumptions

- 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

Outage Assumptions

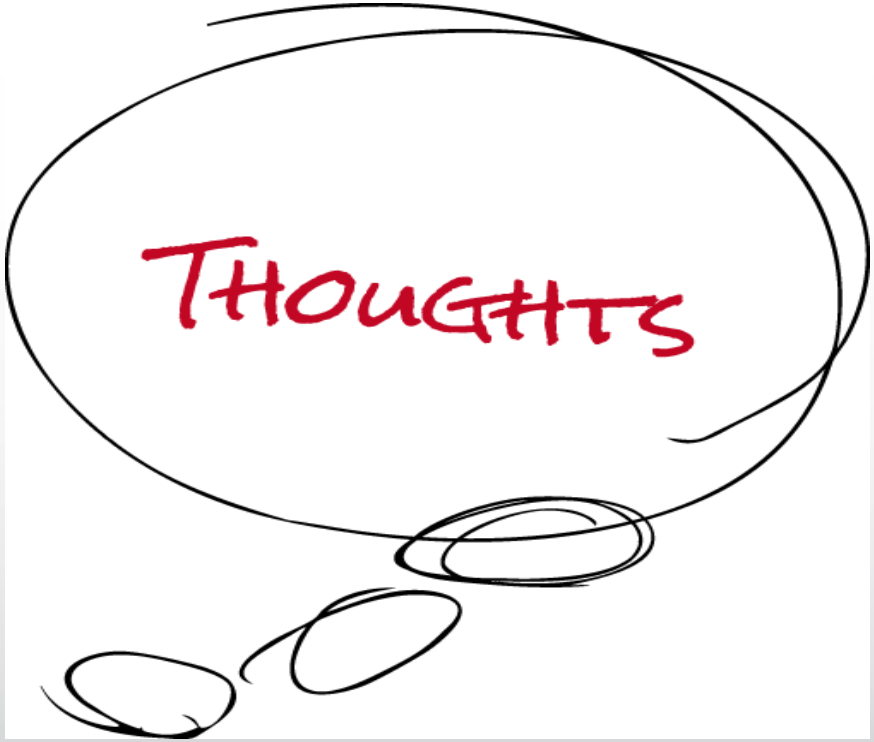
- Impact will be contained to limited resources
  - Office
  - Data Center
  - Servers / Storage
- Relatively short period of time
- Recovery usually doesn't impact entire business

Modern Data Center

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

Today's Assumptions

Are these controls good enough for today's risk?



Preparedness

Future BCP / DR

Why??? - Bigger Threats

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

Recovery

- Can you recover from total data loss?
  - Current Playbook
  - Tested Scenarios
- Can users continue to work?
  - What systems are available first
  - Are mobile applications available and do they work

Can you meet Target RPO/RTO

- Recovery Time Objective (RTO):
  - This is a Service Level Agreement (SLA) setting the maximum period of time that an application will be unavailable in a downtime situation. The shorter the period of time, the faster the recoveries will need to be. Generally, this data includes everything about the operating system, plus applications, configuration data, as well as application data.
- Recovery Point Objective (RPO):
  - This is an SLA setting the maximum amount of data loss that would occur in a downtime or data loss scenario. Frequent backups or near-continuous replication is required to reduce the amount of data loss.

Backups

- Serialization of Backups
  - Are there older file versions available in the event that the new files are encrypted
  - Is the backup system segregated from the production environment

The biggest gotcha that companies are encountering when they get hit with ransomware is that they **haven't had a recent test of their recovery process.**

Backup Best Practices

3-Tier approach to reliable backups

- Day-to-day backups
- Medium-term backups
- Long-term backups

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

Impact on IT

Cultural Impacts

- 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

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

Cost Impact

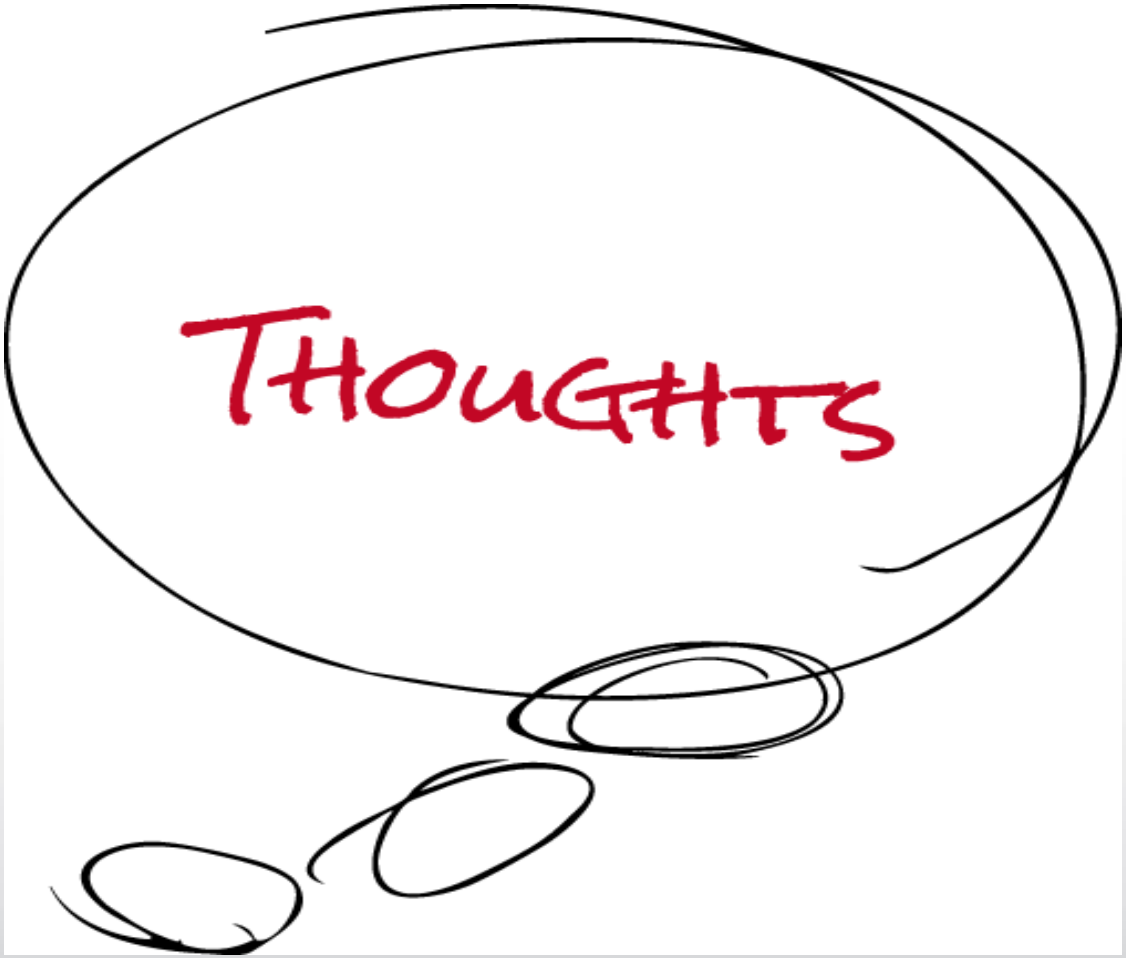
- Forces accelerated adoption of cloud
- Must develop comprehensive cloud strategy
- Must have solid vendor assessment programs
- More complex to manage
  - More vendors
  - Disperse systems
- Harder to provide “unified” user experience

Incident Response

Incident Response

What do you do now????

You get a call at 12:00 am from an Attorney that has clicked on an email and his files are encrypted.


THOUGHTS

Incident Response

- Contact List / Call Tree
- System details
  - Data Flow Diagrams
  - Network Diagrams
  - System Hardware inventory
  - Audit logging
- Incident Intake Report
  - List of breached systems
  - Type of data on breached system
  - Data Loss / Impact
  - Description of the incident
  - Document actions taken

Incident Response Definitions

- Detection – How much time should elapse once a threat is detected
- Analysis – Assessment triage, containment, evidence preservation and recovery
- Recovery – Period of time to restore the environment to normal
- Post-Incident – Detail report from the incident response team to assist in prevention of future incidents

Summary

- Ransomware is real and on the up rise
- Is your data center ready
- Has your backup process been tested
- Incident Response Readiness

Closing Discussion