



Total Networks

Backup, Disaster Recovery: Defining & Managing Your Risk

Dave Kinsey - 5/9/17



Smart Business... also, generally a Compliance Requirement

Shareholders generally do and absolutely ***should*** care that backup & disaster recovery risks are properly managed

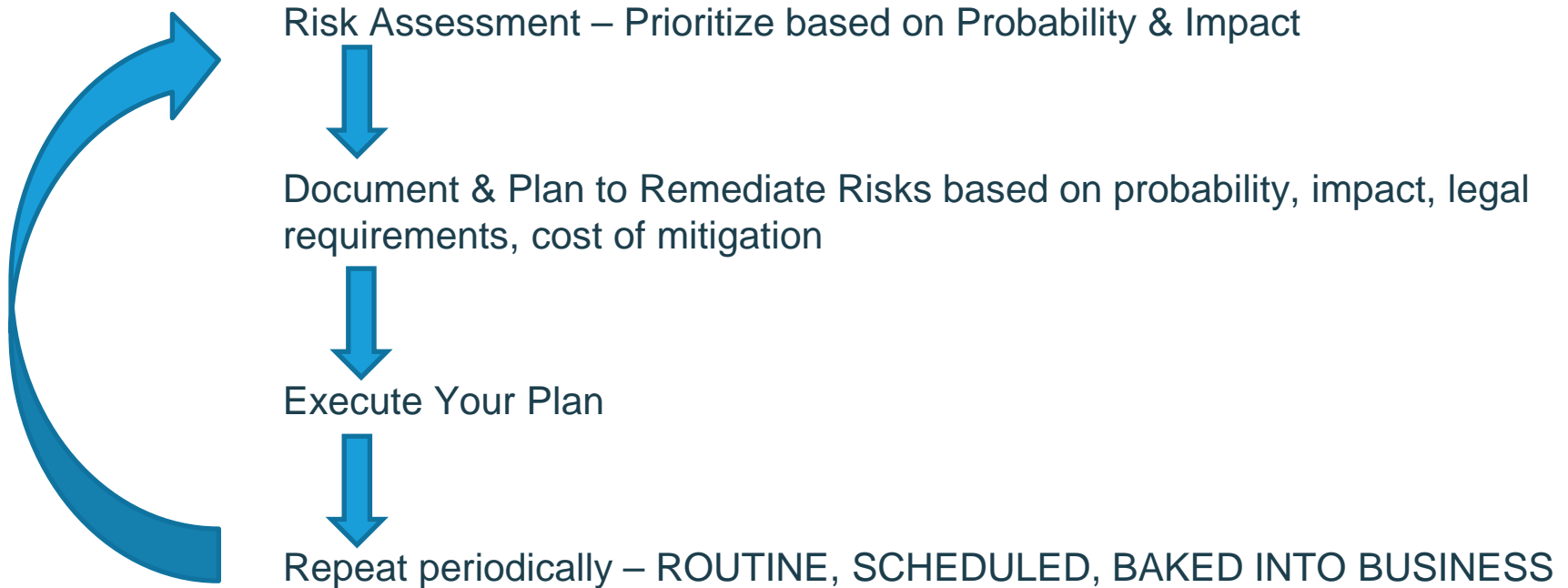
Clients are increasingly validating firms are appropriately managing risks

Many compliance regulations, like HIPAA, ***require*** a data backup & recovery plan

ER 1.1 & ER 1.6 require competence in safeguarding client information



Risk Management Process





How do you define a **DISASTER?**

Are these on your list?

Hurricanes??

Tornadoes??

Fires?

Floods?

Power/network outages

Mechanical or system failure

Human error

Ransomware



Jigsaw

CryptoWall

CryptoHost

CryptXXX

I want to play a game with you. Let me explain the rules:
 Your personal files are being deleted. Your photos, videos, documents, etc...
 But, don't worry! It will only happen if you don't comply.
 However I've already encrypted your personal files, so you cannot access them.

Every hour I select some of them to delete permanently,
 therefore I won't be able to access them, either.
 Are you familiar with the concept of exponential growth? Let me help you out.
 It starts out slowly then increases rapidly.
 During the first 24 hour you will only lose a few files,
 the second day a few hundred, the third day a few thousand, and so on.

If you turn off your computer or try to close me, when I start next time
 you will get 1000 files deleted as a punishment.
 Yes you will want me to start next time, since I am the only one that
 is capable to decrypt your personal data for you.

Now, let's start and enjoy our little game together!

59:47

1 file will be deleted.

[View encrypted files](#)

Please, send at least \$23 worth of Bitcoin here:

12vfQqmMxvDvZdzYHndfURupmcjs8uSpY

I made a payment, now give me back my files!



Remaining 10 Days or 14:398 Minutes

Fee 0.34849 BTC \ 1465365601

Locked 0

Status Locked

Your Computers Files have been Encrypted and Locked!

Your files have been encrypted and are unuseable and inaccessible.
 Don't worry, they're safe, for now.

This is unfortunate although for a small fee all of your Files will be returned to their original location as if nothing ever happened. Simply pay the recovery fee stated on this form and follow the instructions. Once the payment has been received your Files will be returned to normal. Not paying the Unlock Fee to the supplied Bitcoin Address before the Timer runs out means loss of all Files permanently.

The only payment accepted is Bitcoin. If you don't know what Bitcoin is there are instructions on how to obtain Bitcoin and pay the Fee. Just press the "How It Works" Button below to learn how Bitcoin works.

This software checks the Bitcoin Network for the exact payment amount on the Bitcoin address provided. Once the amount is confirmed by clicking "Confirm Payment" your files will be returned to their original locations.

Removing this software causes permanent loss of your files!

This software is the only way to get your files back!

Payment Address:

[Copy](#)

[Review Locked Files](#)

[How It Works](#)

[How to Pay Unlock Fee](#)

[Check Payment Status](#)

Ransomware
had a
BIG 2016

So big, that it has cost
US businesses
upwards of **\$75 billion**
dollars in downtime
and other costs

YIKES!

Ransomware is NOT 100% Preventable

1. Harden defenses: significantly minimize expected infection frequency
2. Minimize impact of infections:
 - Limit/segment/compartmentalize access
 - Ensure high confidence in timely & complete recovery from backup
 - Assess likelihood of data breach & respond appropriately
3. Learn from any incidents for use in ongoing risk assessment & management process

Layers of Defense, Constant Review, Updates

- No “magic bullet” for security
- Many layers and approaches work in concert
- A Harder Target:
 - Well trained people
 - Limited access, eliminate non-business activity
 - Tested, evaluated, maintained defenses
 - Layer upon layer (redundant, with different vendors) defenses
- Security as a process and a culture
- Double-checks, verifications, independent audits

Malware Prevention

Administrative & Technical Safeguards

- Patch systems
- Maintain anti-virus, anti-malware
- Restrict permissions
- Block suspect email and attachments
- Network restrictions: update/maintain IPS/IDS, network AV/AM, block TOR, I2P, restrict unnecessary countries
- PC security (prevent apps running from %APPDATA%, %TEMP% - other)
- App whitelisting
- Provide phishing & other security training
- ***Ensure robust, segregated backups***

Disaster Recovery Plan

Off-site & on-site

File & folder vs. server images

Verify Completeness ON A ROUTINE BASIS:

- Complete inventory of data
- Complete inventory of backups
- Anything missing? By accident? By design? Who approves reviews approves omitting items from a backup?

Recovery Point Objective (RPO) & Recovery Time Objective (RTO)

Recovery Point Objective (RPO):

- How often is everything backed up? How much backup history is retained?
- What CAN I recover?**

Recovery Time Objective (RTO):

- Depending on the disaster, and your plan/capabilities, it could take a LONG time to get back up and running
- Best Case, Worst Case
- WHEN CAN I GET IT?**

Total Networks Approach for On-Site Servers

- Backup & Failover Server on-site (encrypted on-site)
- Image-level backup, generally every hour
- Encrypted backup transfer to two secure data centers (encrypted in-transit and on-site at remote location)
- RPO: from last hourly backup on-site, from last completed off-site replication off-site
- RTO: can be within minutes on-site to standby hardware, in under an hour to off-site
- Verification: monitoring and alerting throughout the day for any failures, daily review of system boot screenshots onsite and off, simulated DR tests performed every 2 months (first step in review process – manual audit of all data, manual audit of backups, nothing new/missing)

Privacy & Ethical Considerations

- Carefully review and vet vendors (and review your client and legal requirements and disclosures)
- Don't let your systems OR BACKUPS cause a data breach
- HIPAA Business Associate Agreement (BAA) may be required and can be a HUGE HELP

It's in the cloud... I don't need backups...

- **Good** cloud applications can *reduce* your backup/recovery risk – especially from obvious disaster. Carries obvious risks as well.
- Diligence & review absolutely still required. Consider separate backup of hosted data. **Total Networks uses Mimecast for backup & DR AND ARCHIVING of both on-premise Exchange & Office 365.**
- Some example risk management questions... do you have risks with...
 - emails accidentally deleted 2 months ago?
 - emails to be placed on legal hold due to a complaint filed against you by a former employee?
 - items on an employee's C: drive?

Beyond Backup & DR Plan... Business Continuity Plan

Think through the various risk scenarios. For EACH scenario (type of issue, expected duration) document your planned response:

- Managing Communication (with employees, clients)
- Everybody Work from Home?
- Physical Meeting Rally Point?
- Testing Your Plan
- Plans Readily Available During Disaster?

Use this thought experiment to refine your plans.

complianceKIT

Total Networks new offering:

- **complianceKIT** provides practical guidance and resources to help businesses manage their security & compliance.
- No matter where you are at in your risk management process, we believe we can help.
- **complianceKIT** provides a framework, templates, coaching, consulting, ***employee training***, and security awareness tools that help business owners succeed.
- **Simulated PHISHING emails**...provide online training to your people (ongoing, plus new hire), see who **still** gets tricked and clicks, provide follow-up training for those folks.

Total Networks' Compliance Consulting Services & Tools

We can help you assess and manage your risk & compliance.
Information conveniently delivered through a web portal

PII PROTECT

Logout
Welcome back, Art
Client: ABC Financial

Home Profile | About PII Protect | Employees | Contact Us

Quick Links:

- Service Provider Contracts
- Security Policies & Procedures
- Security Risk Assessment Documents
- Security Training
- Security Incidents

Service Portal Dashboard

- Policies & Procedures**
Policies and Procedures
Click Here ▶
- Contracts & Documents**
Security Risk Assessment, Service Providers, Disaster Recovery
Click Here ▶
- Track and Document**
Security Incidents and Server Room Access
Click Here ▶
- Education Center**
Videos and Training
Click Here ▶
- Security Risk Assessment**
Perform Your Security Risk Assessment
Click Here ▶

PII Protect Copyright © 2015

THANK YOU FOR YOUR TIME!

Questions?

Dave Kinsey

dkinsey@totalnetworks.com

602-412-5001



Next CLE...

State Bar Convention, Friday, June 16th

“Protecting the Client & Serving the Public in the Digital Age”

3 Hour (ethics)