Resilient IT - Do you have it?

V. Amira Armond
President, Kieri Solutions LLC
CISSP, PMP, MBA, MCSE, ISTQB
amira.armond@kieri.com

Kieri Solutions

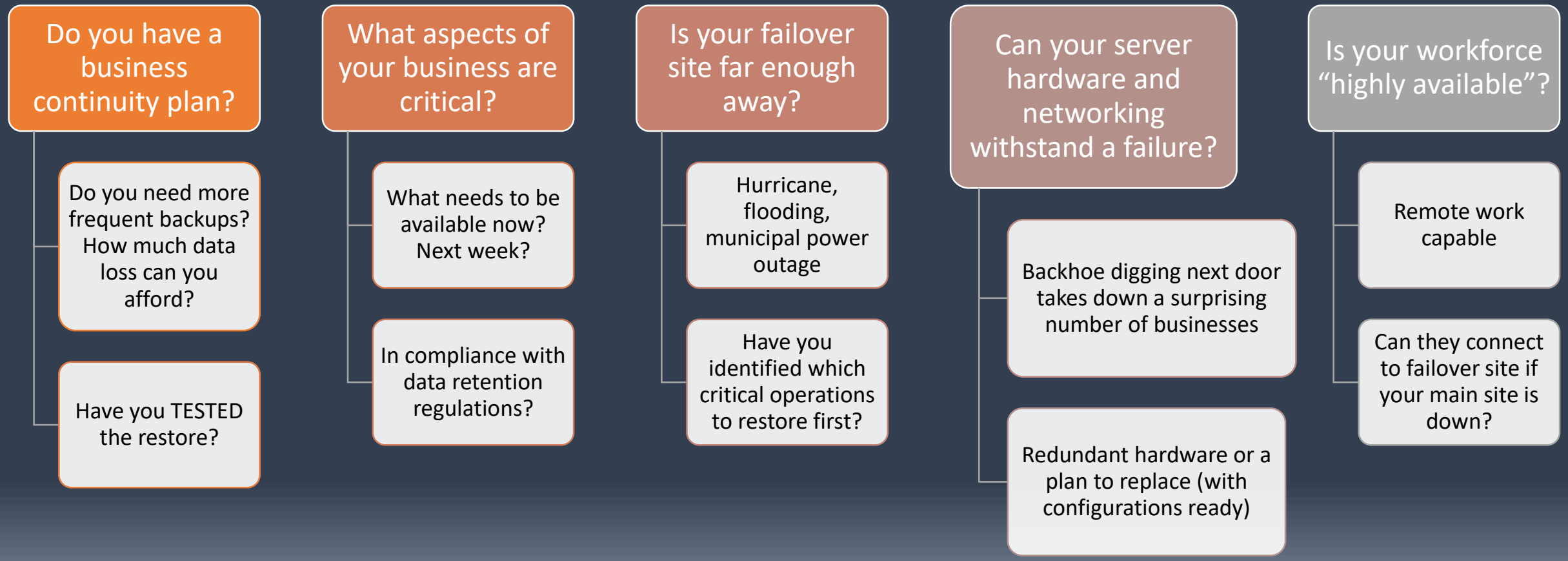
Pareto's Law (80/20 principle)

80% of the desired outcome will be gained by 20% of the effort.

The last 20% takes 80% of the effort.

Understanding that businesses have different risk profiles and resources, it is important to prioritize recommendations by efficiency.

- Tested backup and recovery strategies
- Patching and configurations (enabling the security you have)
- Intrusion protection / antivirus
- Monitoring and penetration testing
- Fully configured firewalls and network segmentation
- High-availability designs



Disaster Recovery / High Availability

Security: Principle of Least-Privilege

- Definition 1: Once you can do everything necessary (ALLOW ALL), restrict other access (DENY X).
- Definition 2: Restrict access to major threat vectors (DENY ALL), then figure out how to do everything necessary (ALLOW X).

Most enterprises use Definition 1. They have a hard time implementing security restrictions after-the-fact. Functionality assumes insecure channels. Increasing security breaks existing systems.

Definition 2 is much harder for threats to penetrate. Threats have to penetrate through multiple layers, rather than gaining full access at the first layer. But it is harder to administer this, requiring more up-front work as systems are implemented.

1

Have you enabled the **existing** security in your products?

- Encrypted client-server communications
- Privilege separation
- Disaster recovery

2

Are your devices and applications missing patches?

3

Are you preventing and detecting abnormal behavior?

4

Not being stupid with passwords and accounts

- **Everyone** fails this test unless they enforce 2-factor or test the hashes for common passwords

Configurations

Are users able to attack-scan your most sensitive database server?

Do you have a monitoring solution that will alert if this happens?

If ransomware attacks your network, could it destroy your backups as well?

Are forensic logs and security events stored for at least a year?

Network Segmentation and Monitoring

Other Considerations

- Would it be front page news if any of your workstations were stolen?
- Outside trusts: Are your cloud-enabled appliances and IoT creating vulnerabilities?
- Can intruders simply plug unauthorized devices into your network?
- Are your users protected against the biggest threats: email and web?

SECURITY

AVAILABILITY

FUNCTIONALITY

RESILIENT IT

www.kieri.com

Consulting services

- Business Continuity / Disaster Recovery Plans
- Identify gaps and solutions
- Step-by-step implementation plans
- Migration / configuration assistance
- High-availability clustering and failover
- Independent test / validate recovery

KIERI SOLUTIONS