When Disaster Strikes

...

Short Survey: https://bit.ly/2kG5KmP

> whoami

Eric Wu – Director, Infrastructure

14 Years at KTX Insurance Brokers and Kanetix Ltd.

Responsible for everything IT related (some unrelated)

> whoami

3 offices

3 data center colocations

10 member IT team

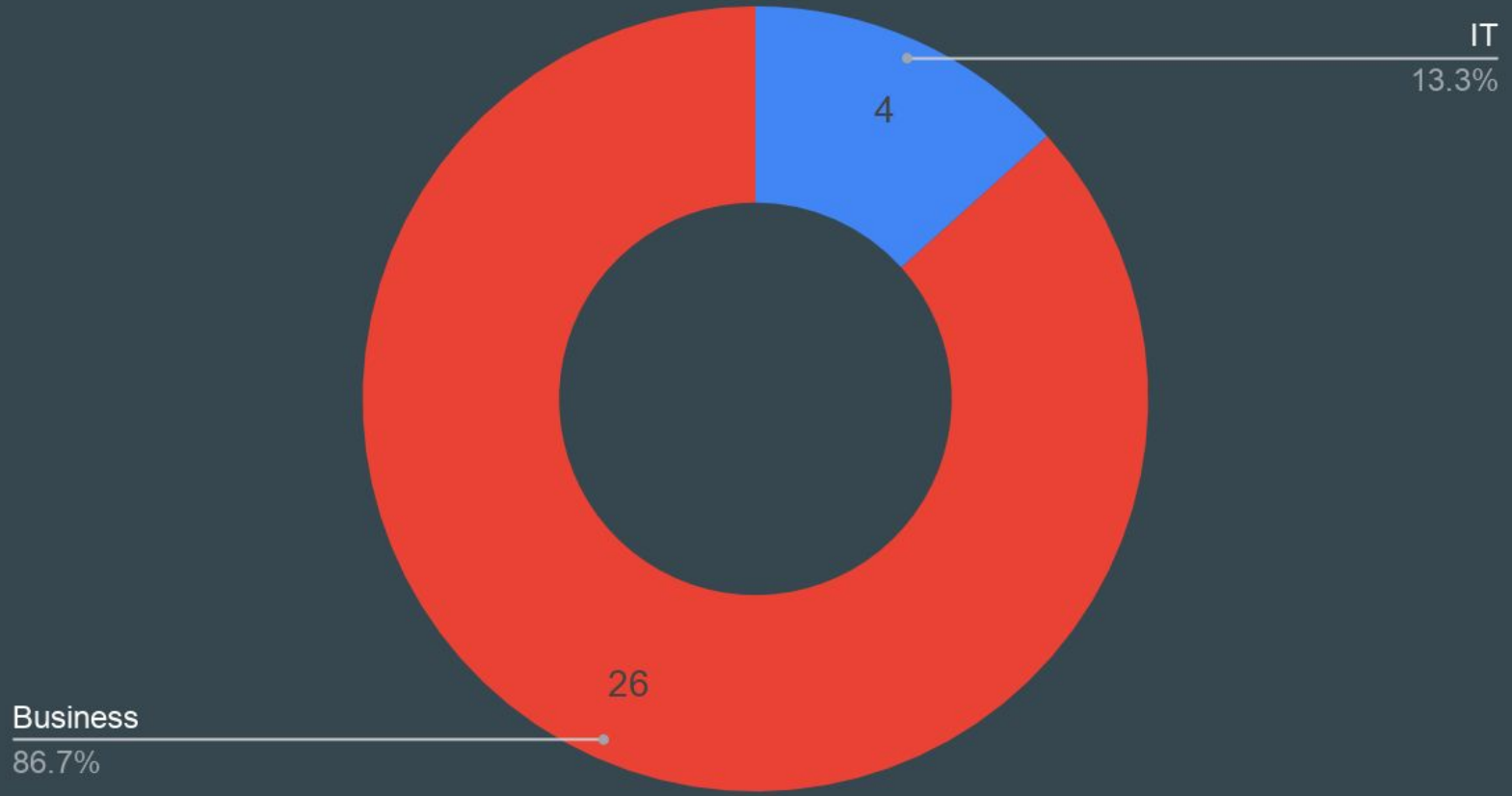
40+ websites (KTX, Kanetix, Insurance companies)

100+ network devices and servers

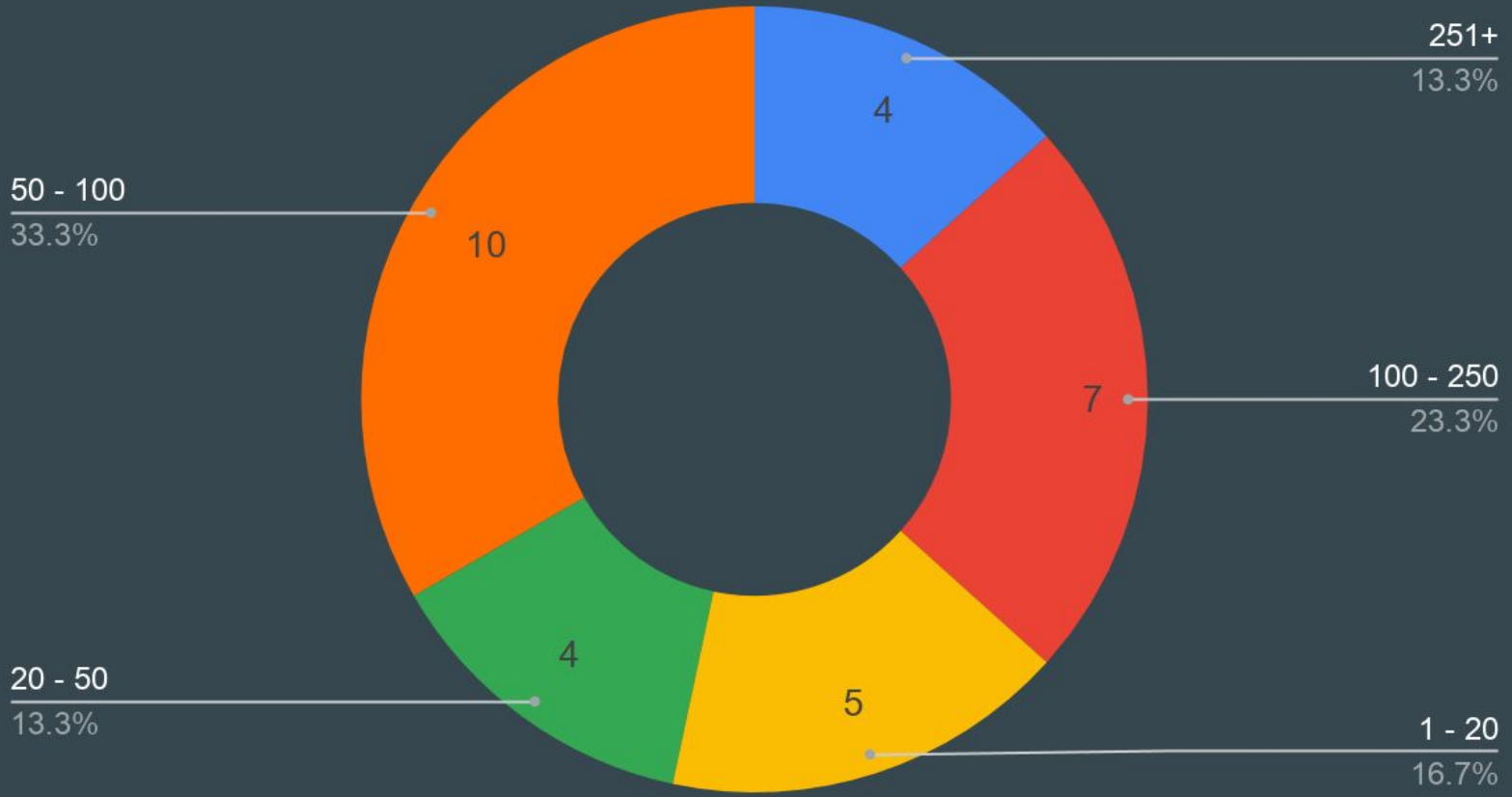
700+ virtual servers

~300 employees and counting

Are you a member of IT or member of Business?



What is the size of your business?



In this session

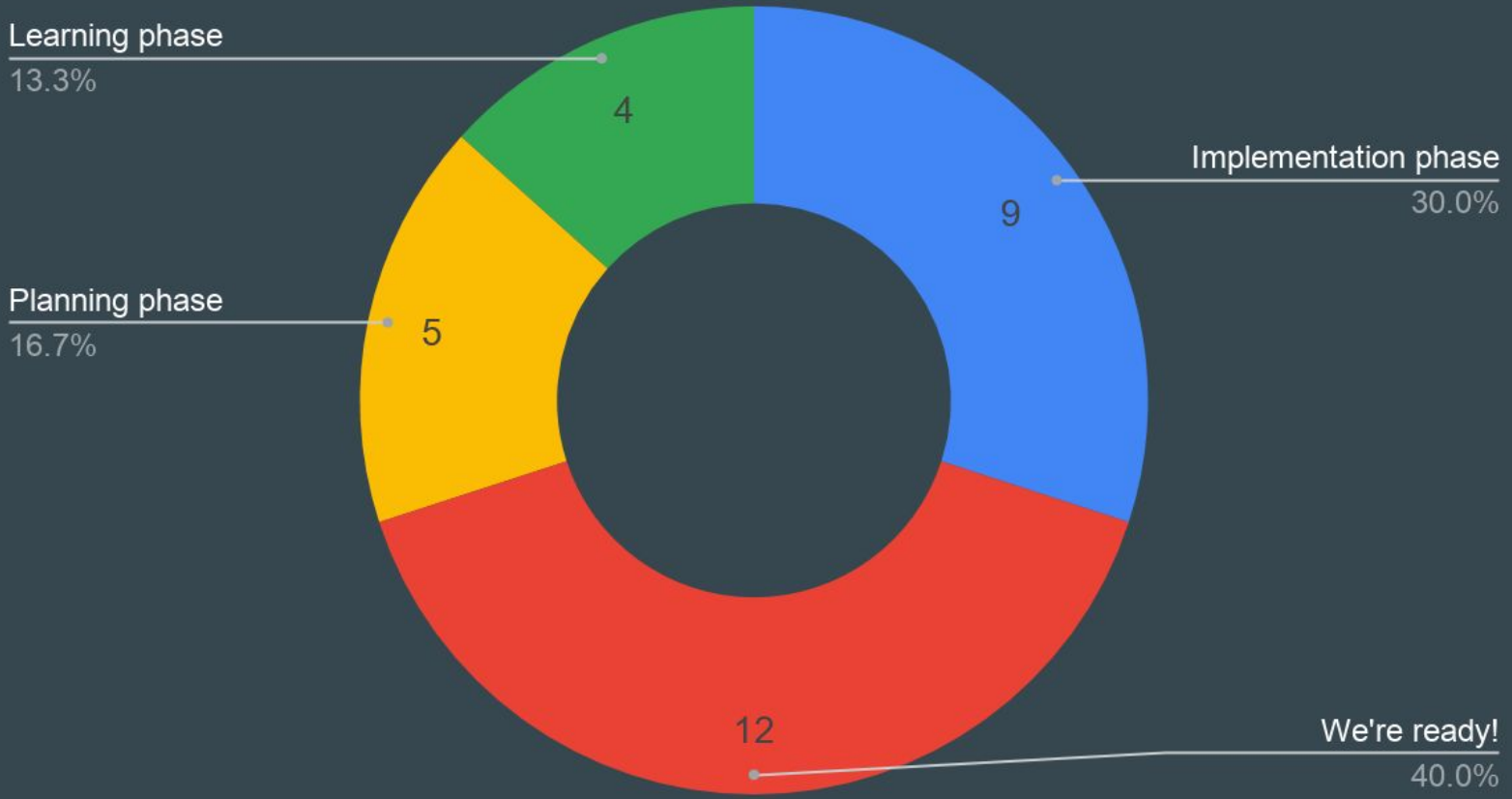
- Identifying critical systems
- Risk analysis
- Understanding systems
- Designing for failure
- Final notes
- Q&A

Whatever can go wrong...

will go wrong.


I am... inevitable.

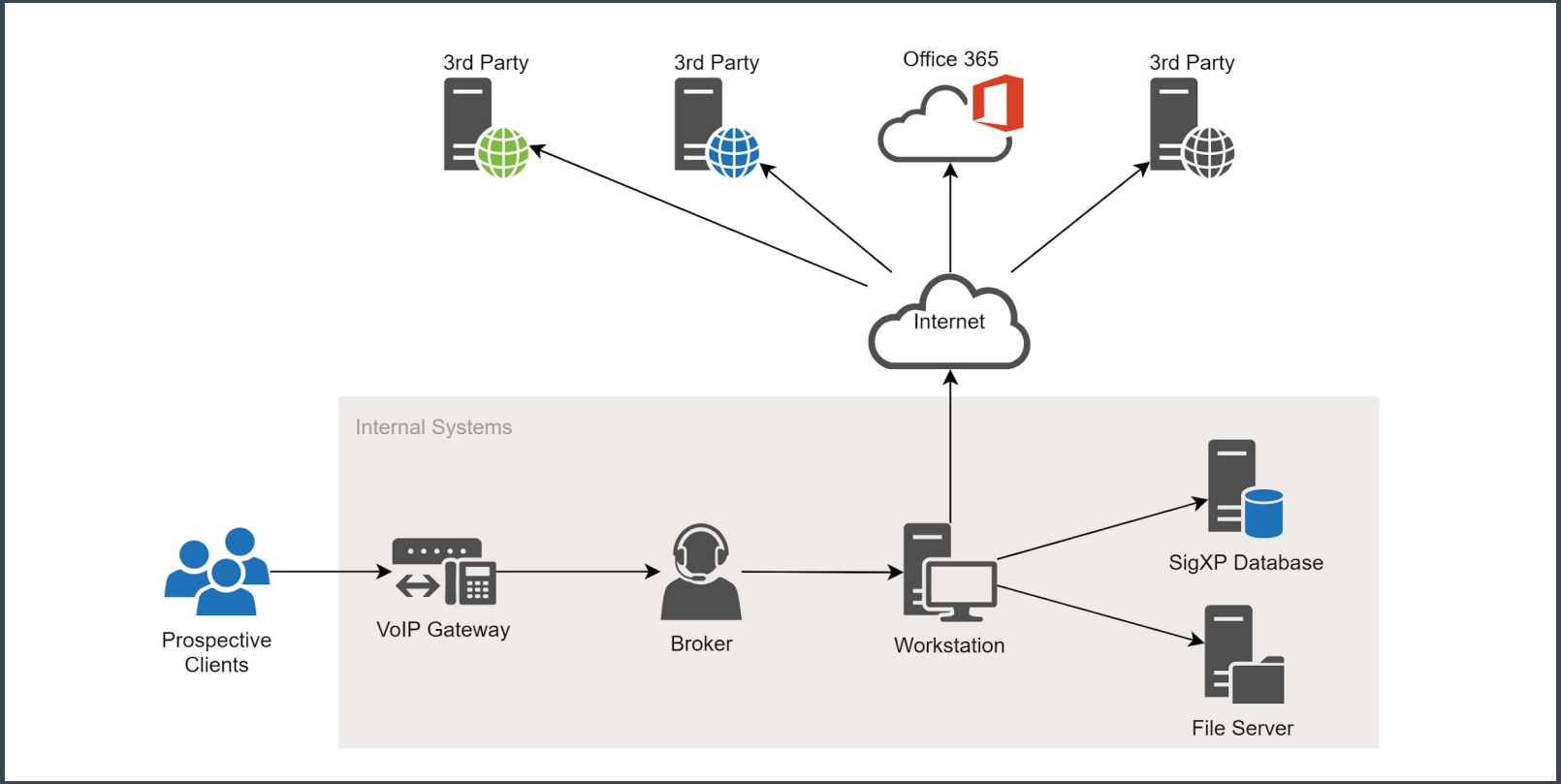
What level of readiness is your IT Disaster Recovery Plan?



In this session

- **Identifying critical systems**
- Risk analysis
- Understanding systems
- Designing for failure
- Final notes
- Q&A

Identifying critical systems



Identifying critical systems

System	Affects Sales	Affects Service	Current RTO	Current RPO
Phone	Yes	Yes		
BMS	Yes	Yes		
Chat	No	Yes		
PCs	Yes	Yes		
...	...	...	...	...

In this session

- Identifying critical systems
- **Risk analysis**
- Understanding systems
- Designing for failure
- Final notes
- Q&A

RTO and RPO

- Recovery Time Objective (RTO) - Time in hours it takes to return IT to operation that is acceptable by business and achievable by IT
- Recovery Point Objective (RPO) - Theoretical maximum data loss since last data backup, measured in hours, that is acceptable by business and achievable by IT

Risk analysis

System	Affects Sales	Affects Service	Current RTO	Current RPO
Phone	Yes	Yes	4 hrs	24 hrs
BMS	Yes	Yes	5 days	24 hrs
Chat	No	Yes	24 hrs	24 hrs
PCs	Yes	Yes	24 hrs	24 hrs
...	...	...	...	...

Risk analysis

System	Affects Sales	Affects Service	Current RTO	Current RPO	Revenue Loss / hr	Risk
Phone	Yes	Yes	4 hrs	24 hrs	5000	Low
BMS	Yes	Yes	5 days	24 hrs	5000	High
Chat	No	Yes	24 hrs	24 hrs	1000	Low
PCs	Yes	Yes	24 hrs	24 hrs	5000	Medium
...	...	...	...	...	...	...

Non-disaster events

- Ransomware
- Damage by disgruntled employees
- Severe data corruption
- Failed software upgrades
- Minor equipment failure
- Data loss

Disaster events

Physical

- Severe equipment failure
- Fire
- Flood
- Earthquake
- Power outage
- Terrorism
- Zombie apocalypse
- Acts of God

Which disaster scenarios should you care about?

In this disaster event...

Are you likely to be in danger?

What's the likelihood that it occurs?

Are your clients in a position to engage with you?

Are your employees capable of travel to another location?

. . .

Disaster scenarios

Physical

- Severe equipment failure
- Fire
- Localized flood
- Earthquake*
- Localized power outage
- Terrorism*
- ~~Zombie apocalypse~~
- ~~Acts of God~~

Setting goals - compromise between IT and business

RTO

- How long to relocate employees?
- How long to get connectivity?
- Complexity of local network setup?
- Complexity of local servers?
- Is employee remote access possible?
- How much revenue loss?
- How much to spend?
- ...

RPO

- Compliance requirements?
- Ideally don't lose any data.
- What technologies can you afford?
- How much work to reproduce lost data?
- How much to spend?
- ...

Setting goals

RTO - 4hrs

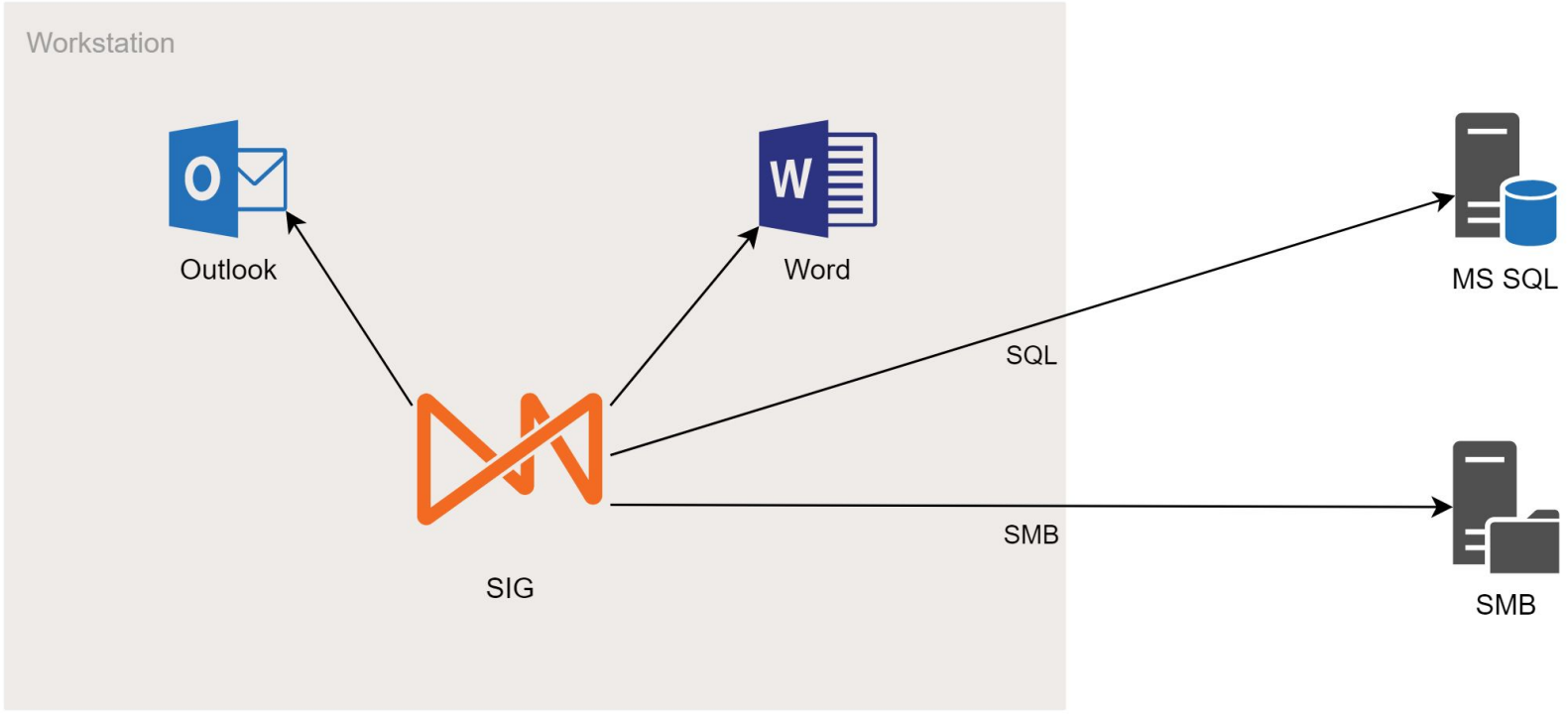
RPO - 4hrs

Require protection to outside of province.

In this session

- Identifying critical systems
- Risk analysis
- **Understanding systems**
- Designing for failure
- Final notes
- Q&A

How does SigXP work?



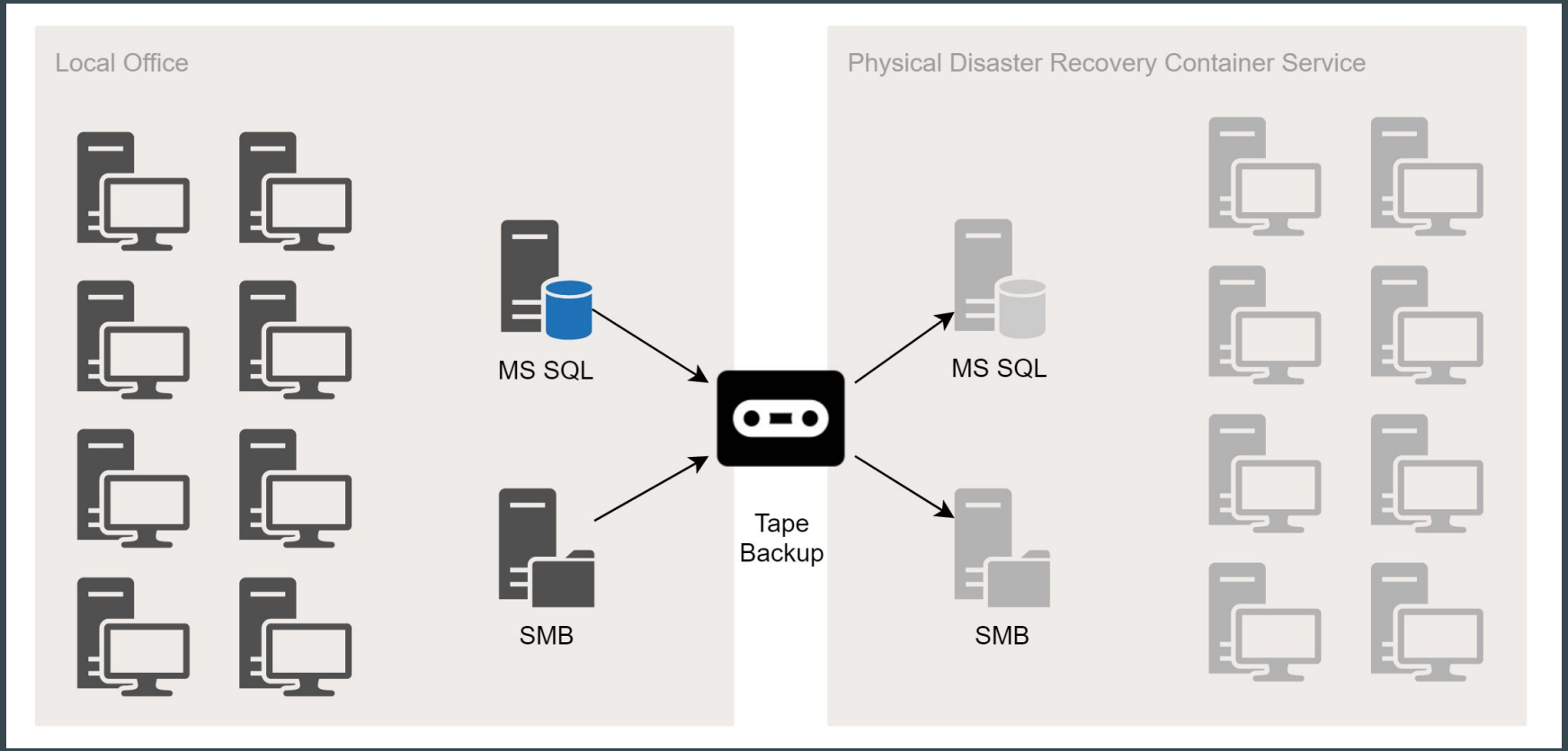
Facts and constraints

- Broker needs access to a computer
- Requires Windows to run all applications
- Outlook and Word must be desktop applications on the same workstation
- Majority of data stored within MS SQL server
- SIG application files stored on central SMB file server
- MS SQL and SMB are not designed for high latency access
- Newer version of MS SQL and SMB perform better with high latency access
- MS SQL and SMB allow asynchronous replication
- ...

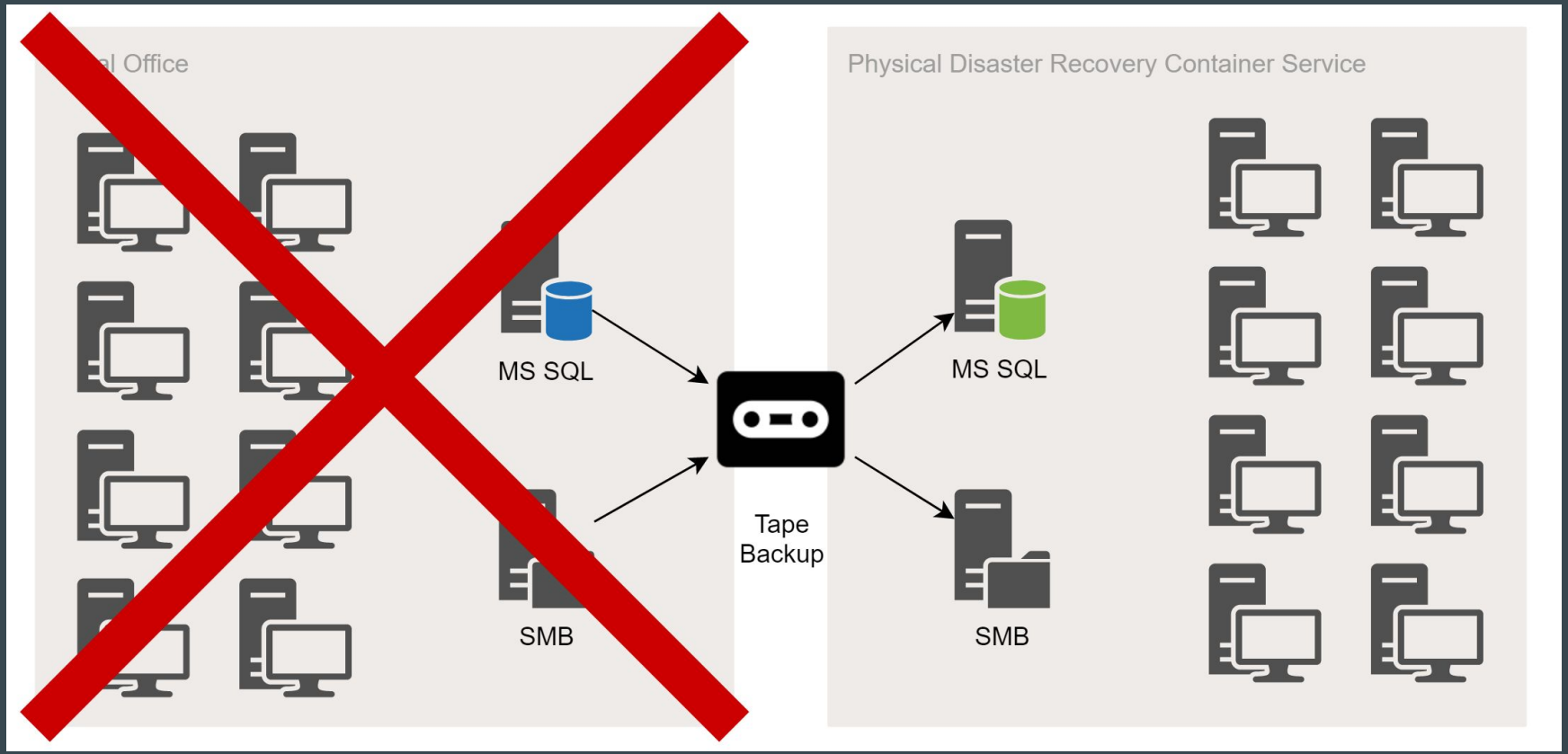
In this session

- Identifying critical systems
- Risk analysis
- Understanding systems
- **Designing for failure**
- Final notes
- Q&A

Traditional disaster recovery



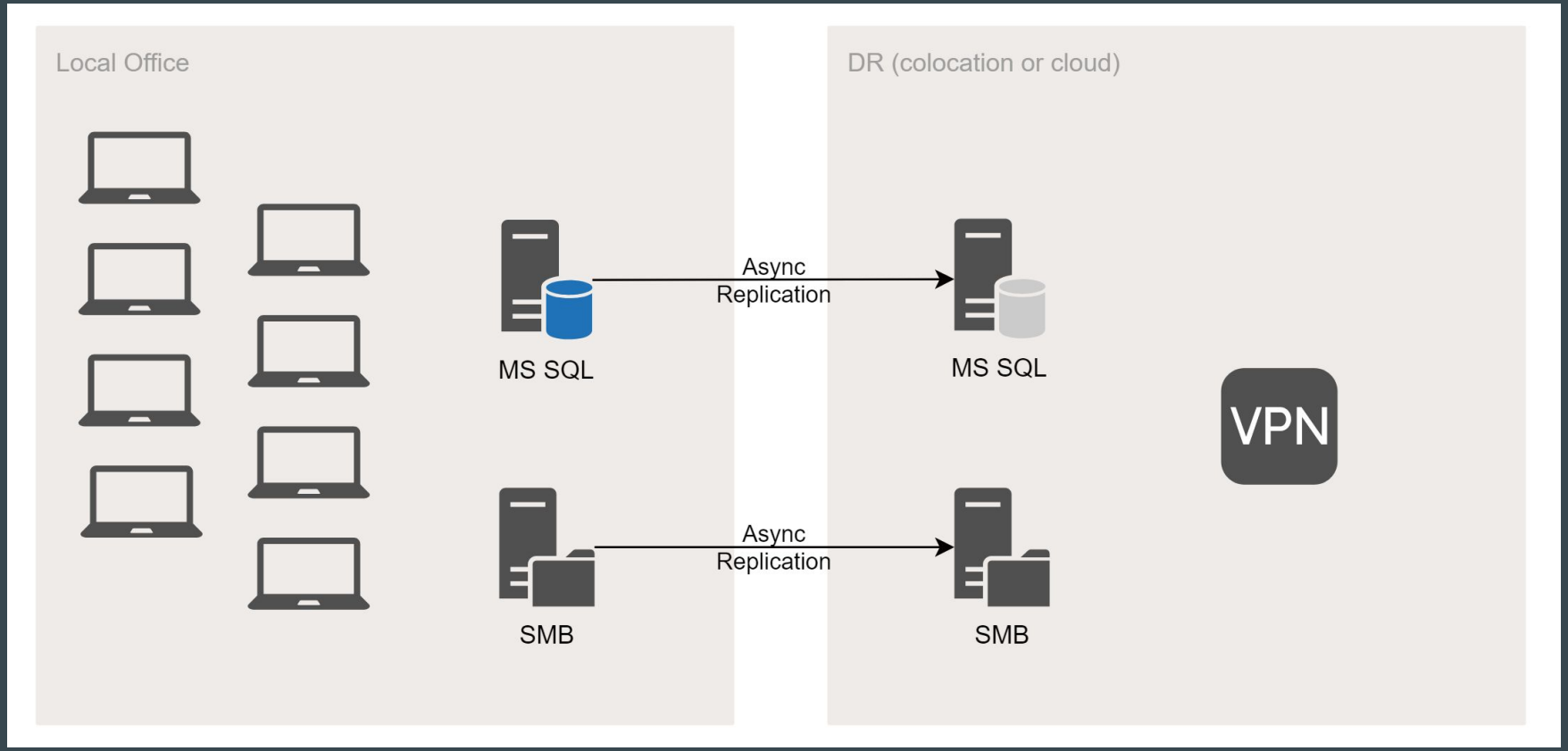
Traditional disaster recovery



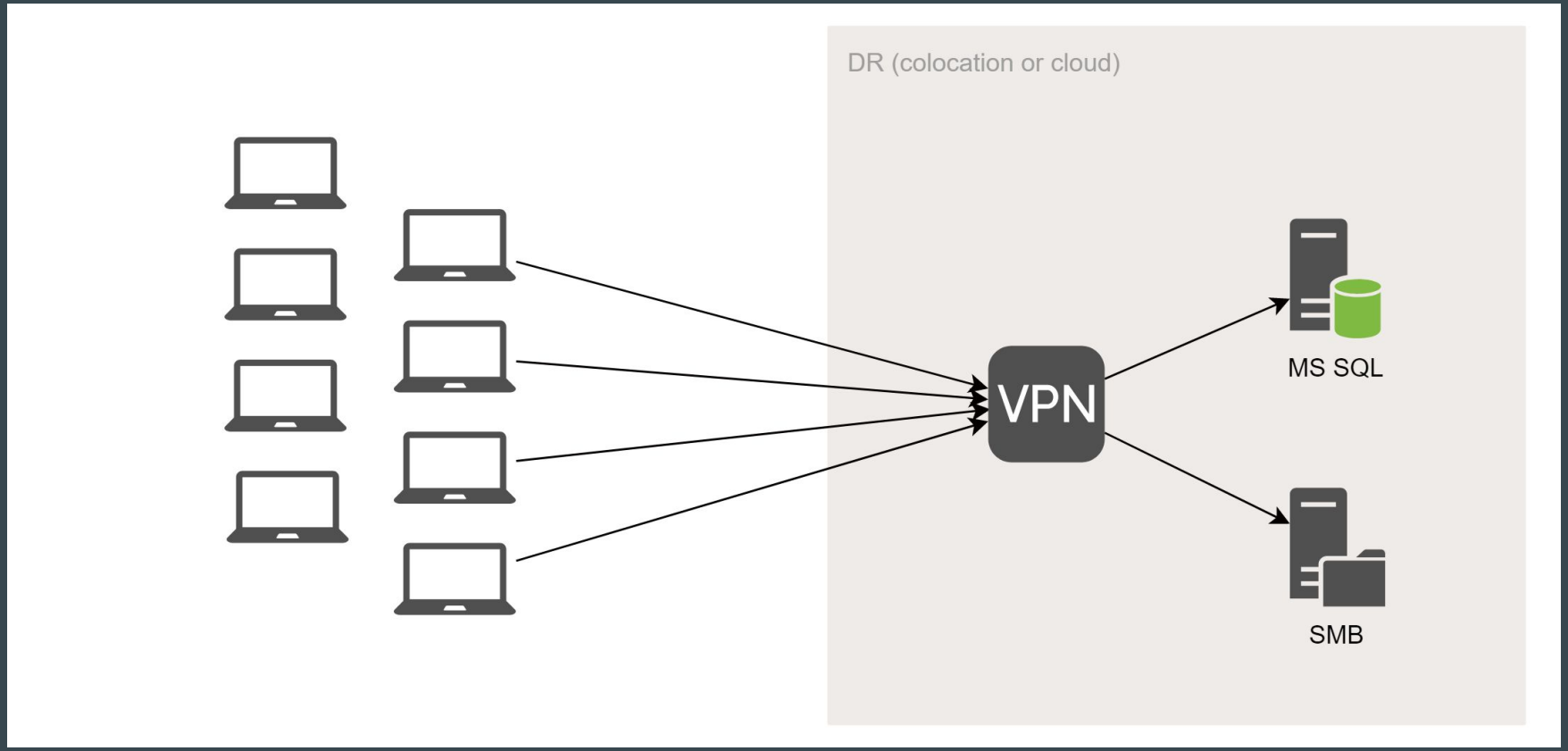
Traditional disaster recovery

- Measured RTO: 24hr+
- Measured RPO: 24hr+
- Temporary physical space
- Temporary equipment
- Technologically simple to execute
- May require employees to travel
- Can be costly to keep reserved
- Manual processes
- Backups may not restore the way you expect

Alternative disaster recovery (remote workers)



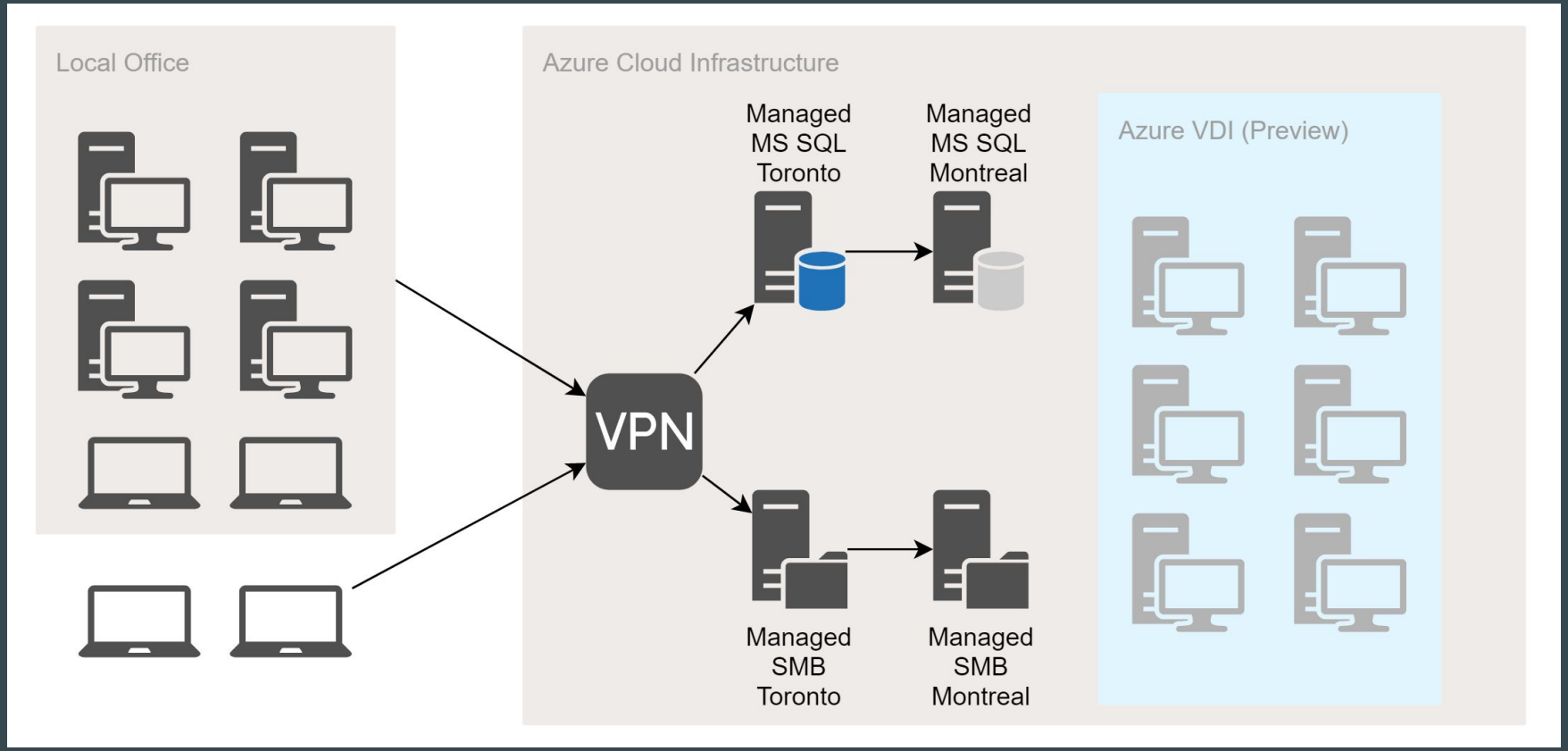
Alternative disaster recovery (remote workers)



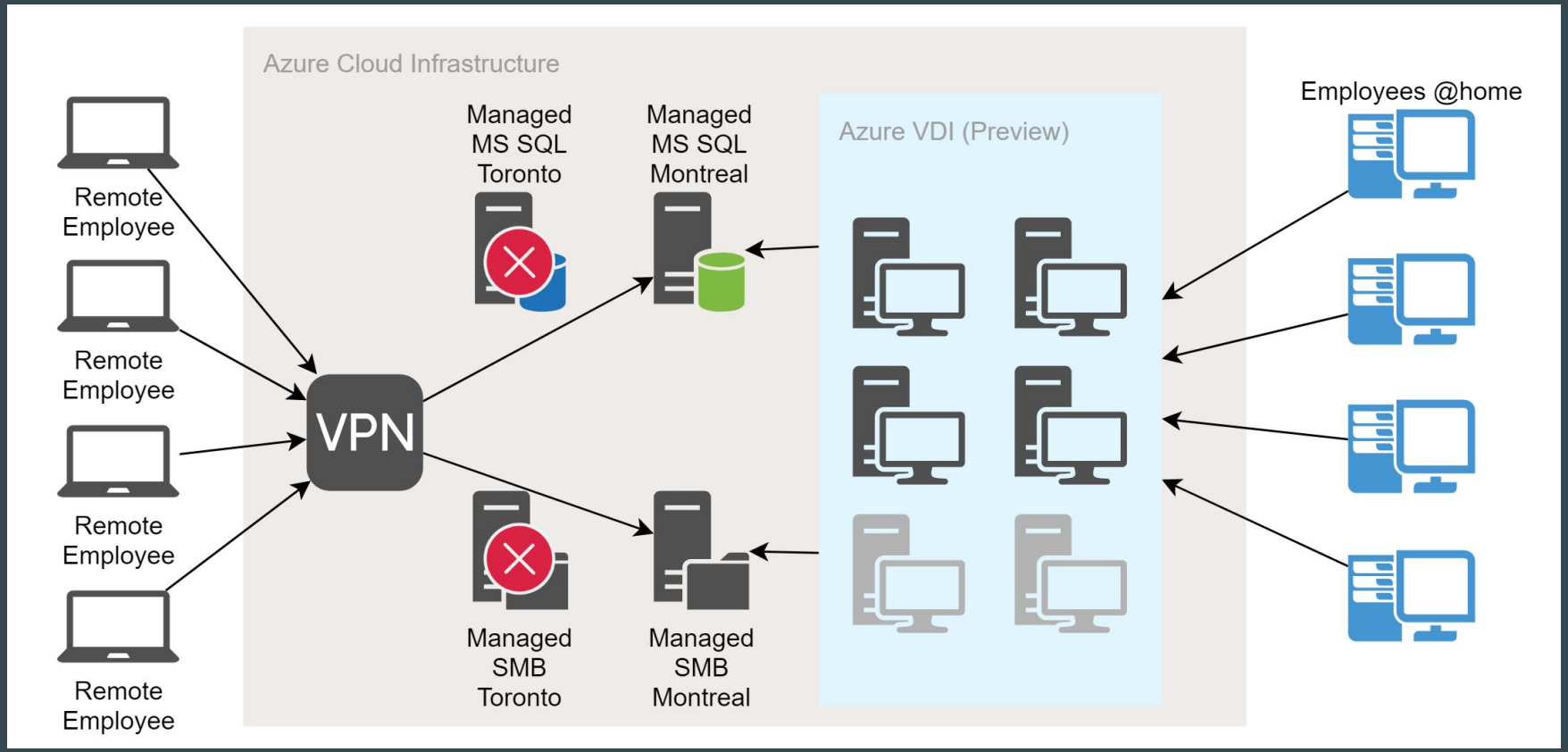
Alternative disaster recovery (remote workers)

- Measured RTO < 4hrs
- Measured RPO near zero
- Assumes a mobile workforce
- Minimal data loss during switchover
- Employees can work from home
- Minimal manual processes
- Reduced cost
- Can reduce costs further using backup to cloud only, spin up servers and VPN when needed programmatically

Experimental DR design



Experimental DR design



Experimental DR design

- Measured RTO near zero (or under 30min for desktop users)
- Measured RPO near zero
- Replaces on-premise DB and File servers with highly available PaaS
- Majority of plan can be programmatically built for automation
- Minimal to no data loss during switchover
- Employees can work from home
- Accommodates mobile and desktop workforce
- Requires reliable and fast Internet connectivity at office

Don’t over engineer

You may say that you’re a small business and are happy with sending backups to cloud, then deal with rebuilding services there later.

- That’s totally fine!
- This may be the cheapest method yet!
- Automate your service builds ahead of time with build scripts!
- RPO depends solely upon your backup frequency

Don’t forget backups!

- Replication does not replace backups!
  - Malware and ransomware
  - Garbage in, garbage out
- Take DB and file backups to cloud
  - Object storage provide versioning and retention policies
    - (Azure Blob, AWS S3, Google Cloud Storage)
  - Encryption at rest is free!
  - 3.5 cents/GB standard storage or 1 cent/GB coldline monthly cost

That great...

but what about just achieving HA?

Achieving HA

On Premise

- Two SQL servers in a cluster
- Two file servers in a cluster (requires AD)
- Double the licensing costs
- More servers to maintain
- Create HA in your network!

Cloud

- Leverage Platform as a Service (PaaS)
- Azure can provide HA service for you
- Azure can replicate data across the world
- HA service within one region to lower costs
- Create HA in your network!

4.1 Billion

Internet users as of Dec 2018

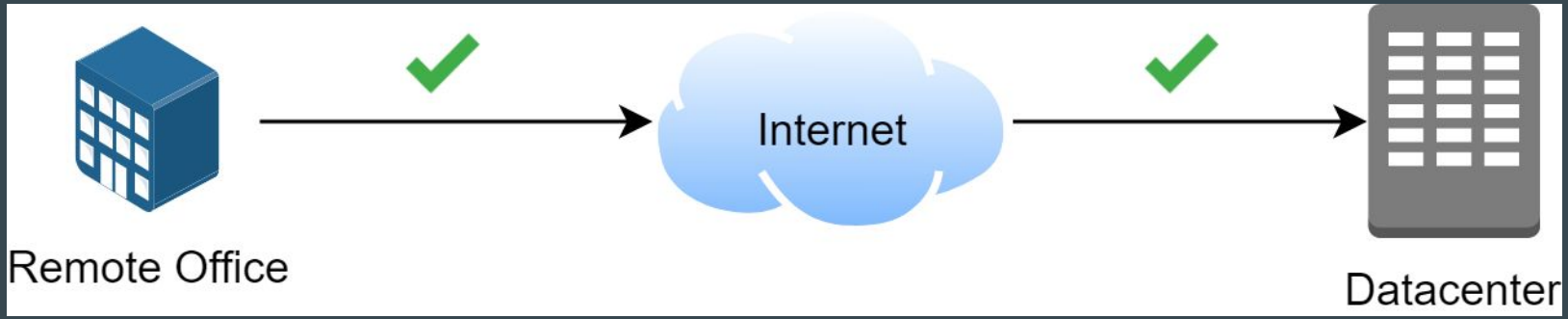
Internet outages

Internet routing issues

Site to site network outages

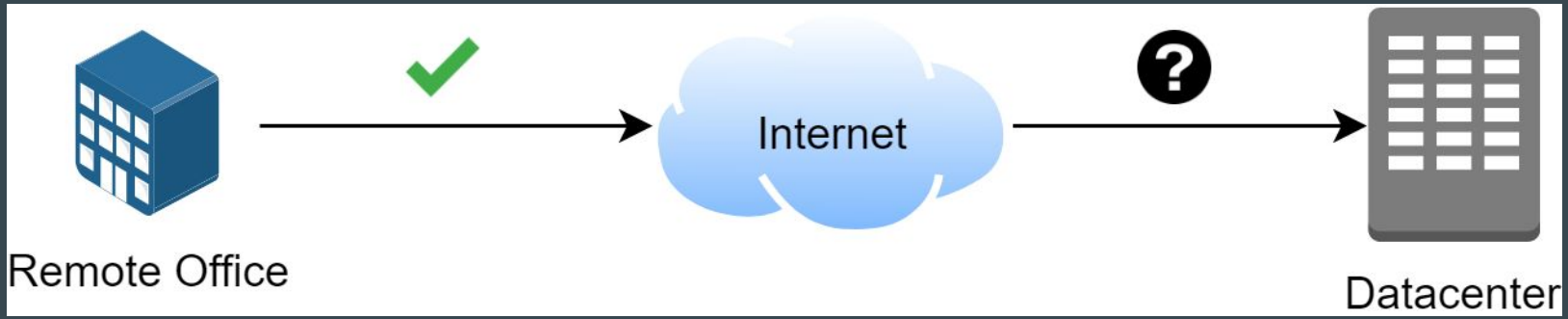
Network equipment failures

Internet connectivity



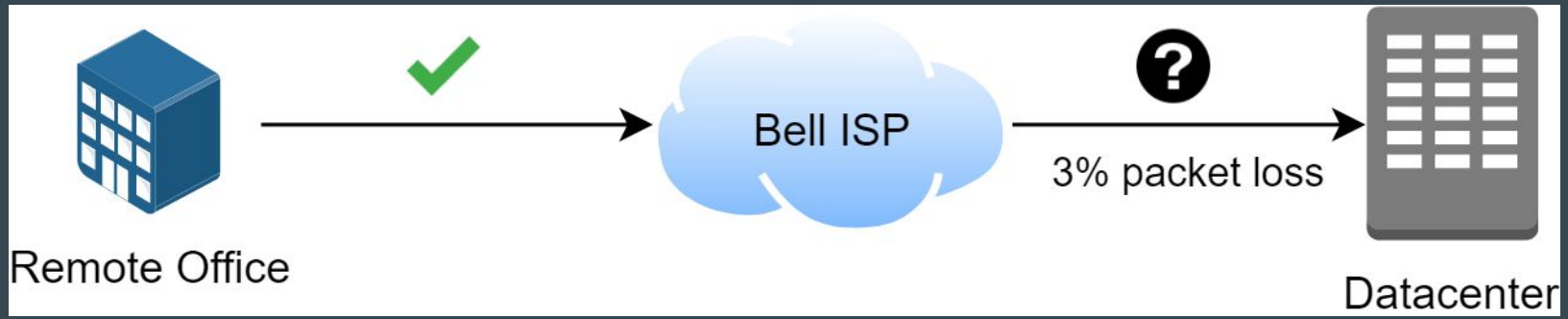
Normal Operation

Internet connectivity



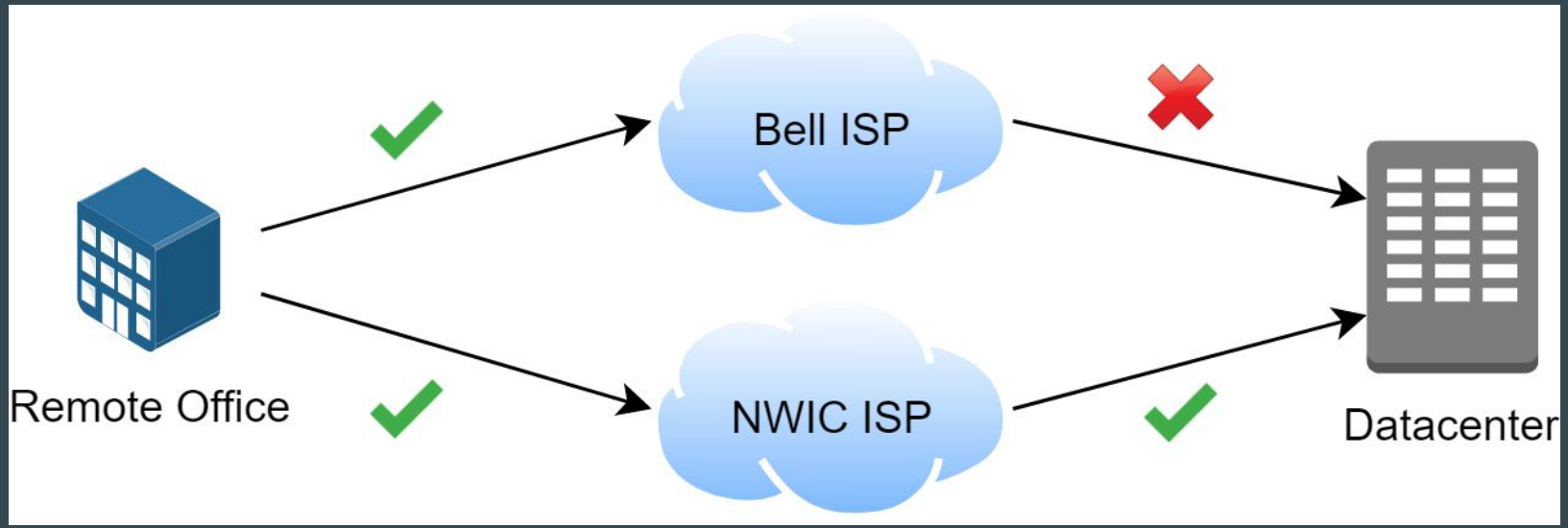
Issues talking only to datacenter?
No problem... 4hr SLO.

Internet connectivity



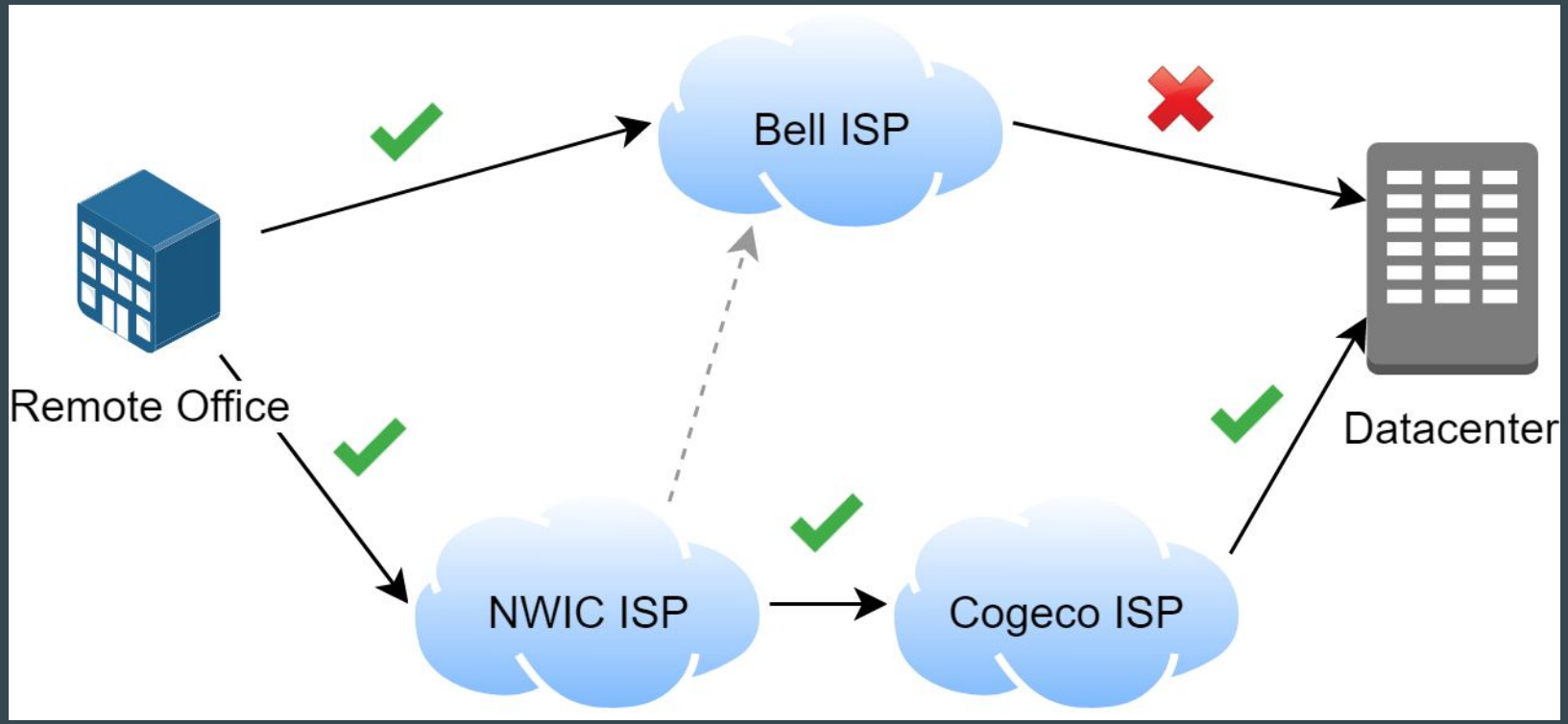
Packet loss on Bell core router.
And they didn't know?
For 5 days! I'm so shocked!
(sarcasm)

Internet connectivity



Redundant deployment?
But NWIC peers with Bell!

Internet connectivity



Internet connectivity

- Two distinct paths to the Internet
  - Some providers lease fiber and network from larger players
  - Fiber lines may take same physical paths into the building
  - Ask provider to send ‘traceroute’ to your critical services
  - Good connection to Internet may not mean your traffic gets to destination
- Routers can handle two or more Internet connections
  - Ensure it supports session pinning in active-active scenario
  - Active-passive is good too, but higher temporary failure
- Latency is key
  - High latency on a fast connection to your remote resource results in slow transfer rates
- 4hr SLA/SLO may not mean much
  - If you have two distinct connections, low cost connections may suffice

Internal networking

- Active passive routers
- Spread access to multiple network switches to reduce failure impact
- Explore Wifi as alternative to wired networking
  - 802.11ac, 802.11ac wave 2, and future 802.11ax
  - Spread APs to multiple switches
  - Failed switch results in zero outage
  - May require professional deployment
- Enterprise price may not equal enterprise reliability
  - Brands like Meraki cost 10x of disruptors like Ubiquiti
  - We've experienced faster Wifi and less outages with Ubiquiti
  - If you don't need enterprise control, save some money

I’ve got that down...
And I use managed cloud services.

Now what?

Understand your cloud services!

- What is their SLA and related compensation model?
- How do they handle high availability?
- How do they handle Disaster Recovery?
- How do they handle backup?
- How do they practice their security?
- Where do they keep their data?
- Is it easy to export your data?
- Is your exported data in industry standard formats?

Understand your cloud services!

Lack of transparency or lack of these capabilities is a red flag.

Find another vendor!

In this session

- Identifying critical systems
- Risk analysis
- Understanding systems
- Designing for failure
- **Final notes**
- Q&A

Plan, test, fix, repeat

- Start with tabletop exercise to highlight deficiencies in your plan
- Address deficiencies and create test scenario
- Isolate DR systems from production and test
- Repeat until satisfied
- Repeat periodically


Click Me.
You Know You Want To.
Wait...
Maybe You Shouldn't?
Nah, C'mon.
Do It Already!

The big red button

- IT DR plan must be part of Business Continuity Plan
- Must clearly define responsibility
- Must clearly define backup personnel
- Must clearly define communication channels
- No one person should make the decision alone
- Prematurely activating IT DR plan can result in data loss

Putting it all together

- Disaster is not if, but when!
- Understand workflow and identify critical systems
- Perform risk analysis of critical systems
- IT and Business set RTO and RPO targets
- Create and test DR proof of concepts, leveraging cloud
- Connectivity is key, ensure it is well planned and tested
- Always scrutinize cloud managed services
- Add IT disaster recovery into BCP
- Test everything!


I am... inevitable.

I am... Iron Man.

Q&A

Eric Wu, Director of Infrastructure

Kanetix Ltd. and KTX Insurance Brokers

eric.wu@kanetix.ca or ewu@fluffy.io

Copy of slides:
https://github.com/ericxw/public-speaking