



Round Table meeting: Outsourcing PCI-DSS

April, 5 2011

Round Table meeting: Outsourcing PCI-DSS

Agenda:

18.00 – 18.30	▪ Welcome & coffee	Isaca Belgium
18.30 – 18:45	▪ Introduction	Isaca Belgium
18:45 – 19:45	▪ A case study of PCI-DSS outsourcing	David Callebaut
19:45 – 20:00	▪ Questions & Answers	All
20:00 – 20.15	▪ ISACA topics: agenda - events - ...	Isaca Belgium

Outsource PCI-DSS

perceptions, fictions, and realities

The views and opinions expressed within this presentation are solely my own and do not necessarily reflect the position of my employer, nor are they intended to be taken as business, security, financial or legal advice.

Delhaize group in a nutshell



Delhaize group in a nutshell

United States:

1.607 stores
USD 18.9 billion revenues (EUR 14.2 billion)
Food Lion, Hannaford, Sweetbay

Belgium, Luxembourg:

792 stores
EUR 4.6 billion revenues

Greece:

216 stores
EUR 1.4 billion revenues

Delhaize Group :

2.732 stores
138.000 associates
Revenues: EUR 19.9 billion
Operating profit: EUR 942 million
Net profit (Group share): EUR 514 million

Rest of the World:

Romania, Indonesia
117 stores
EUR 233 million revenues

Agenda

What is PCI-DSS?



PCI-DSS version 2.0



AB Vassilopoulos Case



Costs and conclusion



Q&A

Agenda

What is PCI-DSS?



PCI-DSS version 2.0



AB Vassilopoulos Case



Costs and conclusion



Q&A

What is PCI? - overview

- Consist of 3 standards
 - PCI-DSS (12 requirements)
 - PA-DSS (13 requirements)
 - PTS
- Started in 2006
- Driven by VISA, Mastercard, Amex, ...
- *Loosely based on ISO27002*

What is PCI-DSS?

requirement overview

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel

Agenda

What is PCI-DSS?



PCI-DSS version 2.0



AB Vassilopoulos Case



Costs and conclusion



Q&A

What is PCI-DSS version 2?

- Released in October 2010 – effective January 2011
- Mostly “clarifications” and “Additional guidances”
- Requirements changed:
 - 6.2 (establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities)
 - 6.5.6 (testing requirements for “high” vulnerabilities identified)
- First references to virtual machines

PCI-DSS Tricky requirements

1.1.6: review firewall and router rule sets at least every 6 months

5.1.1: ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

6.1: Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

8.5.8: Do not use group, shared, or generic accounts and passwords, or other authentication methods

10.6: Review logs for all system components at least daily.

Agenda

What is PCI-DSS?



PCI-DSS version 2.0



AB Vassilopoulos Case

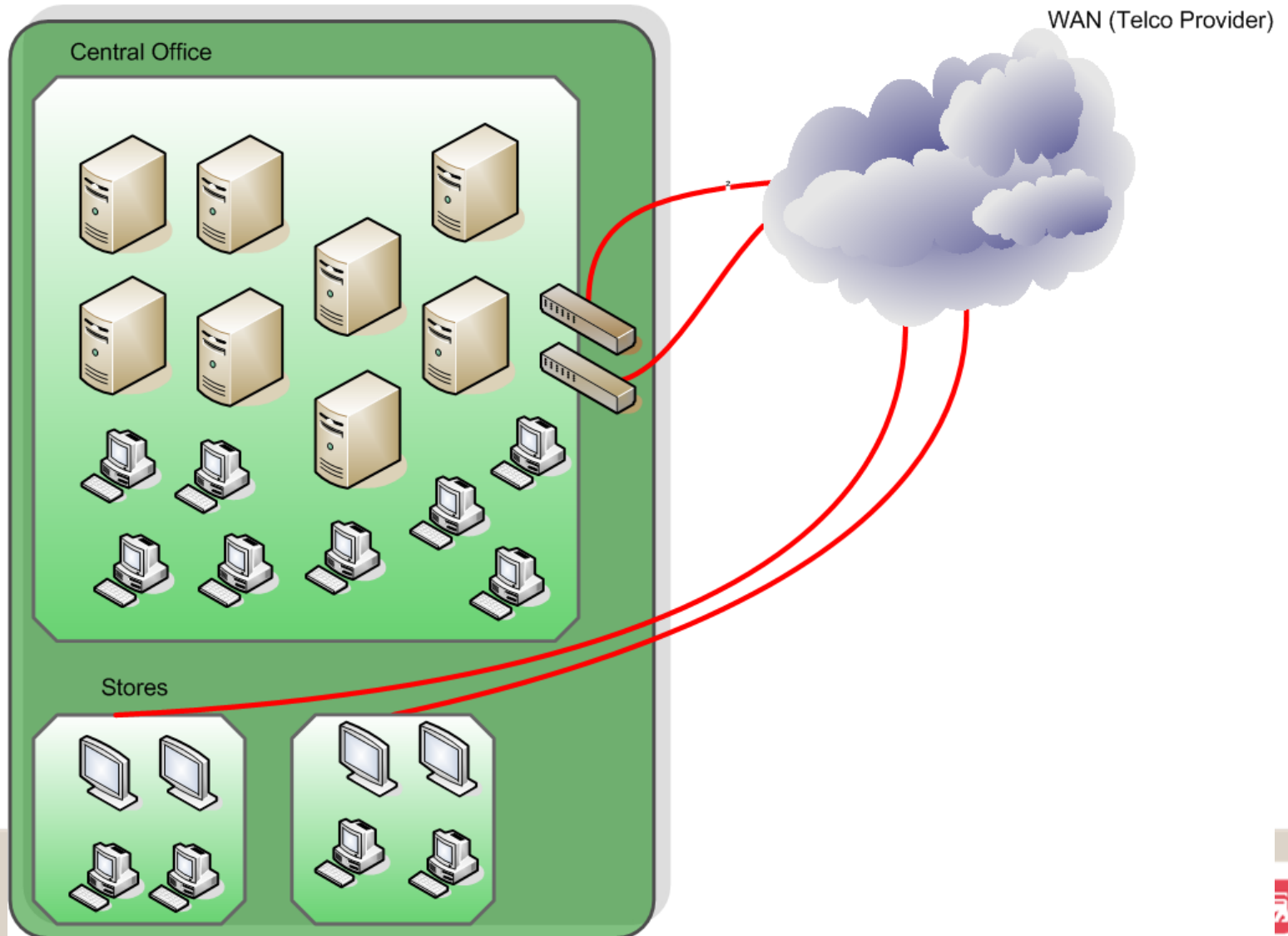


Costs and conclusion

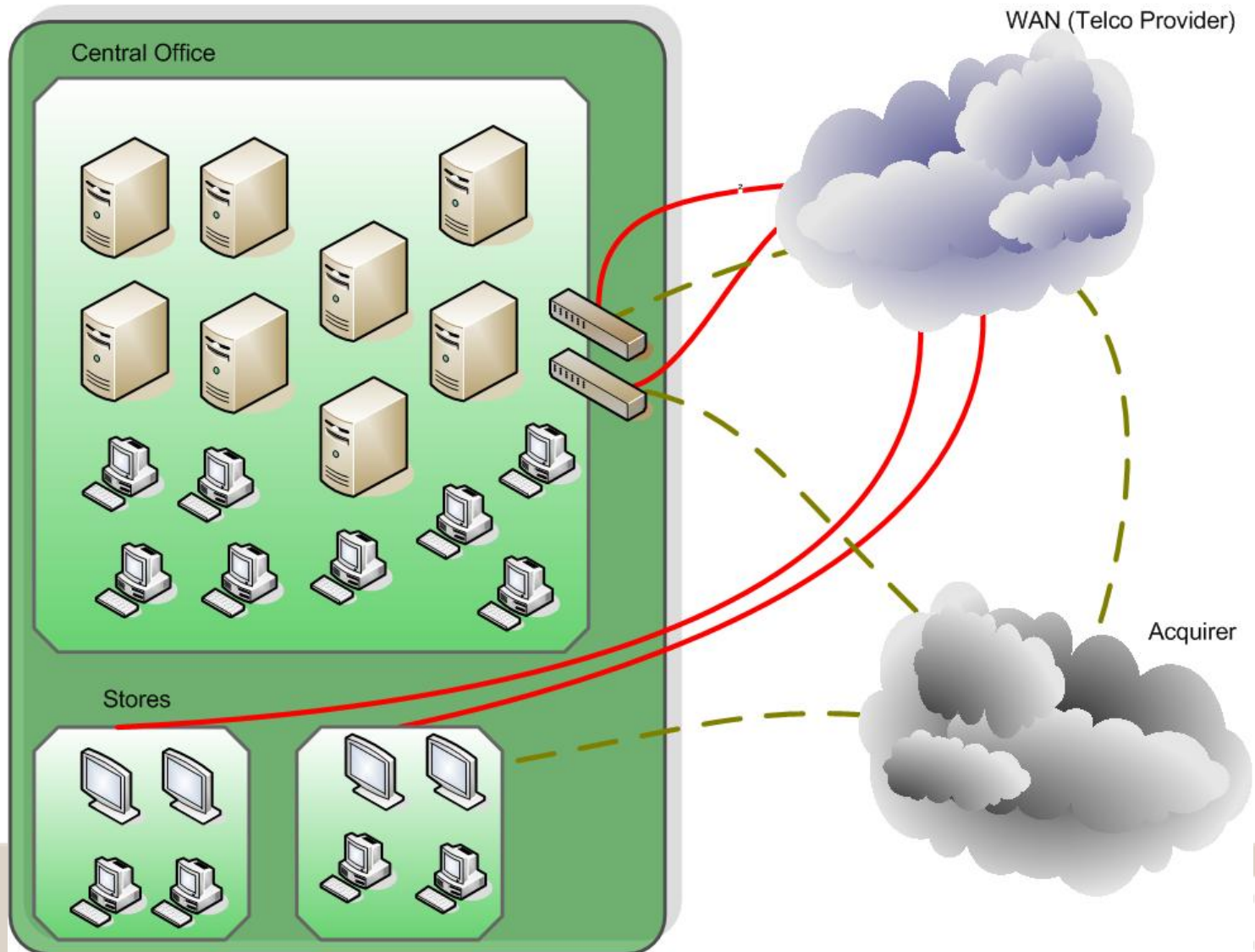


Q&A

Retail typical architecture



Retail typical architecture



Then PCI-DSS kicks in...

- Move systems with CHD into separate, secure areas
- Shield off any other links or entry points
- Buy/install new technology
- Enforce standards and policy on security controls
(Shouldn't they already been there?)
- You do you best...

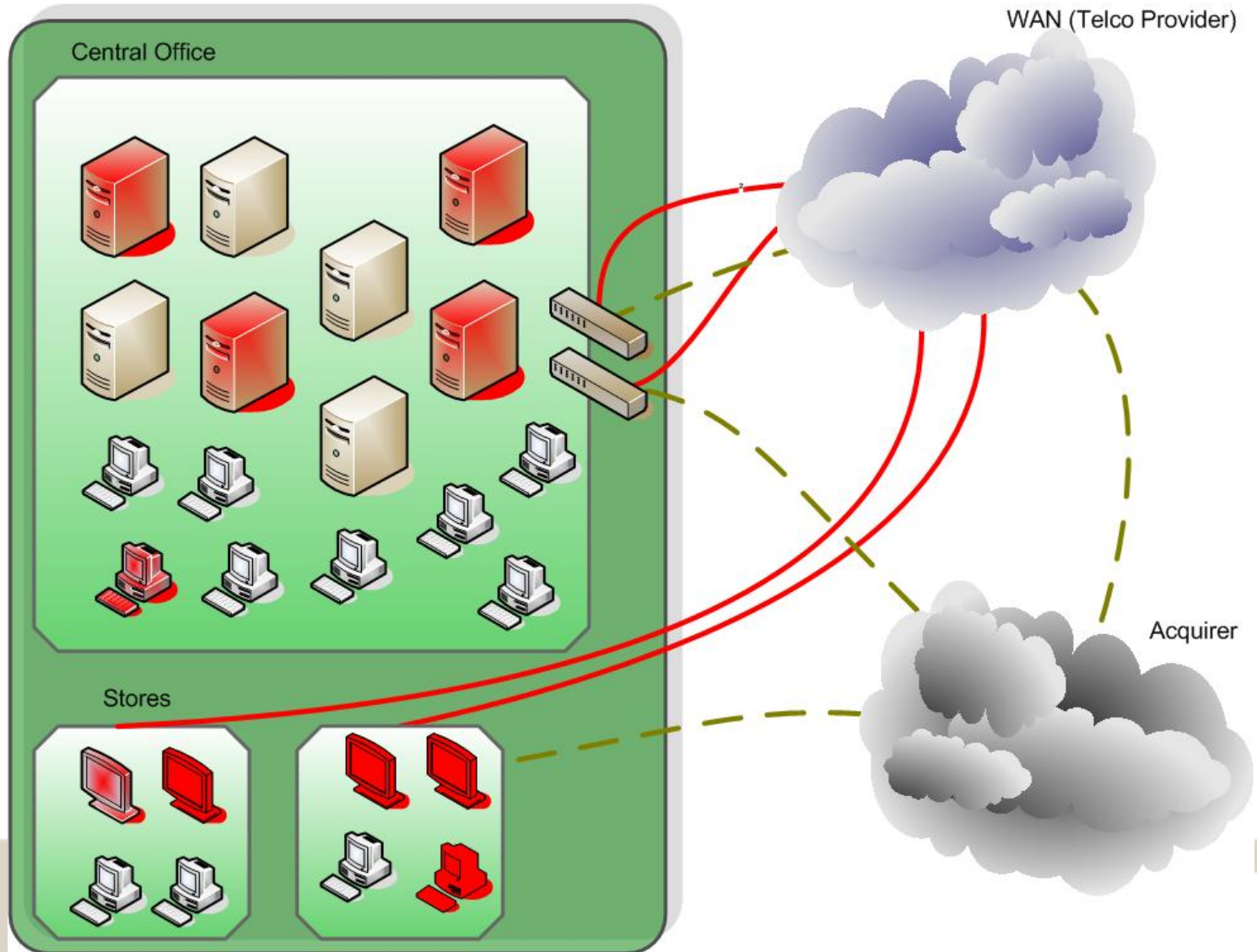
We are the PCI-DSS...

... Resistance is futile



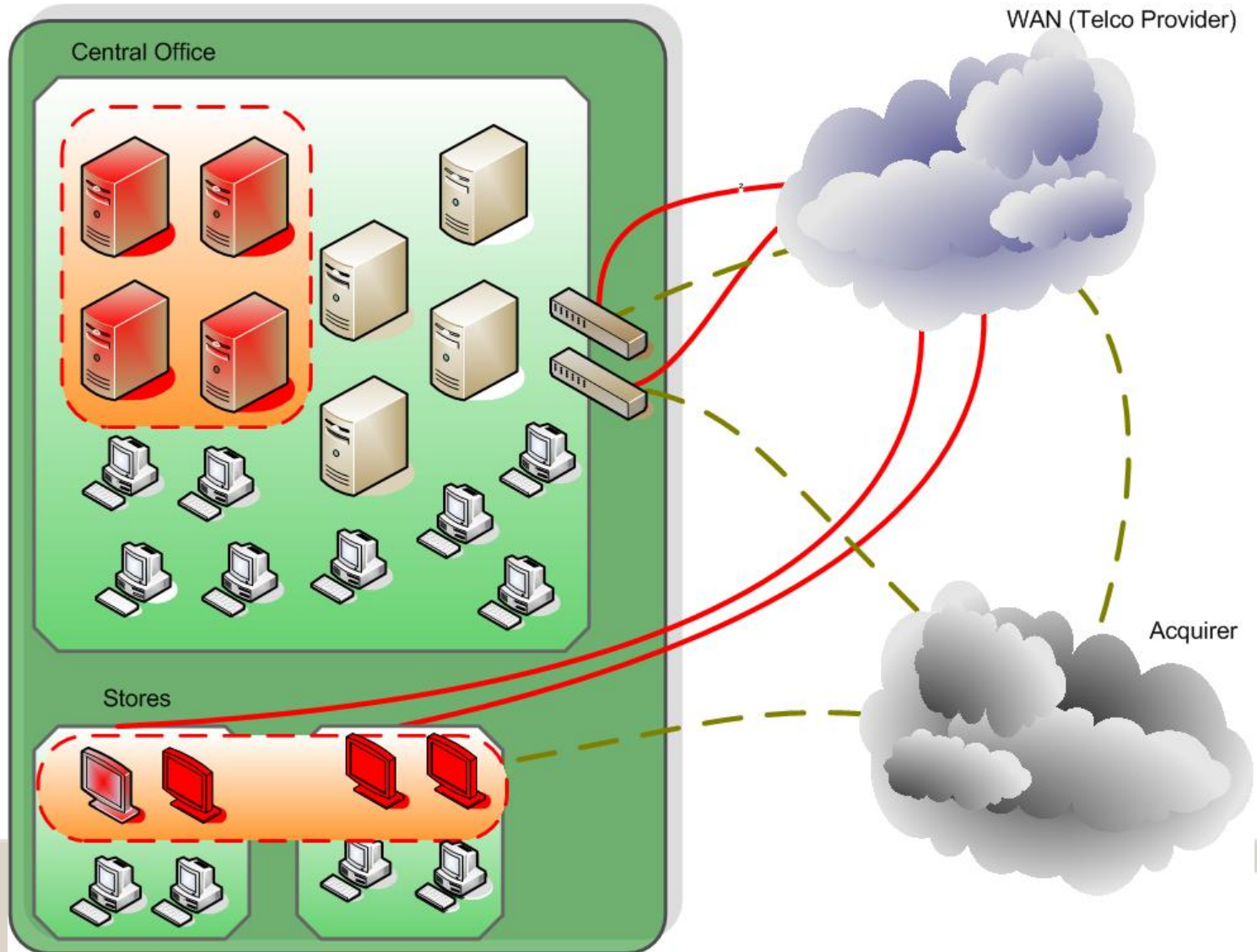
PCI-DSS is here!

Identify the systems and processes involved



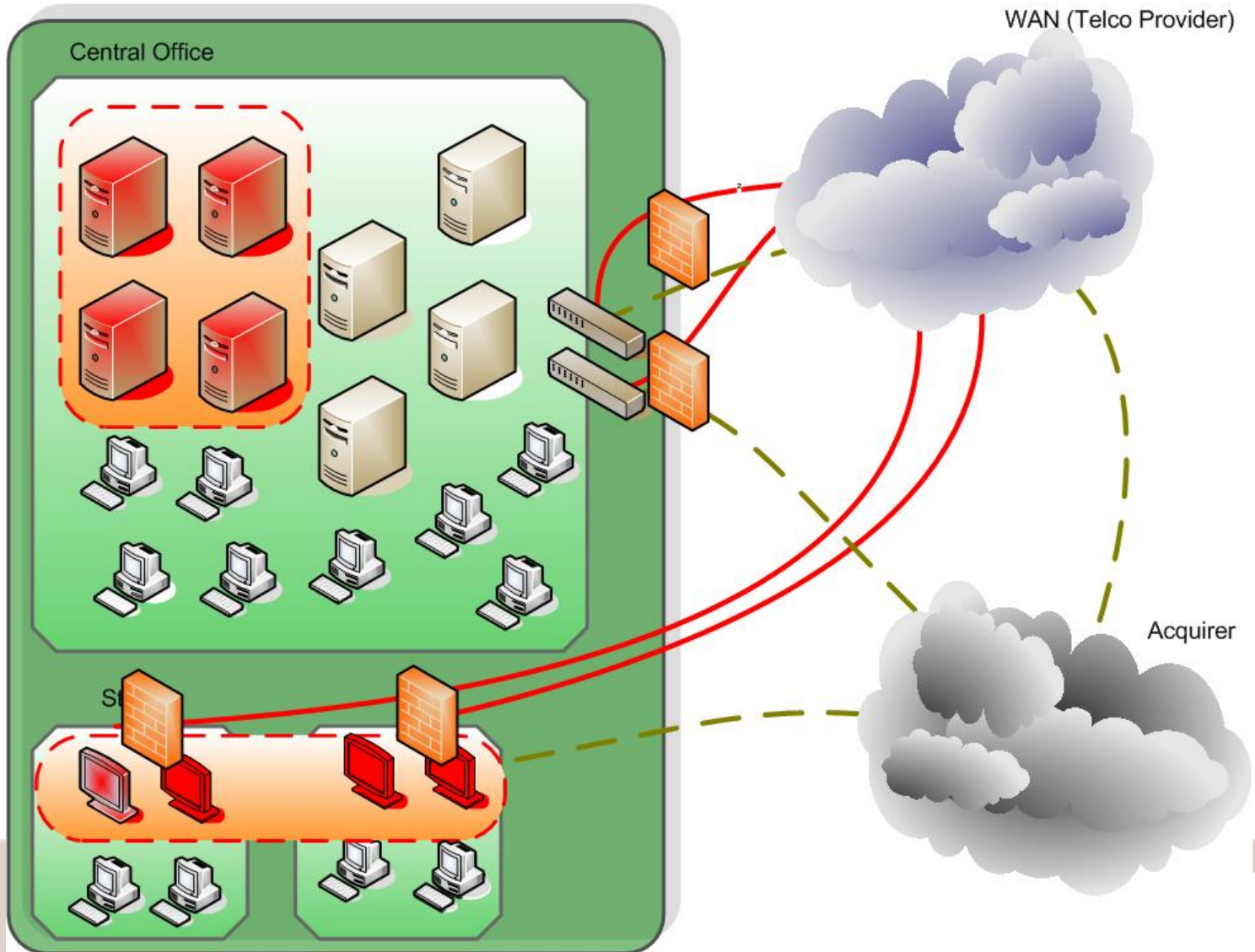
PCI-DSS is here!

Concentrate and split



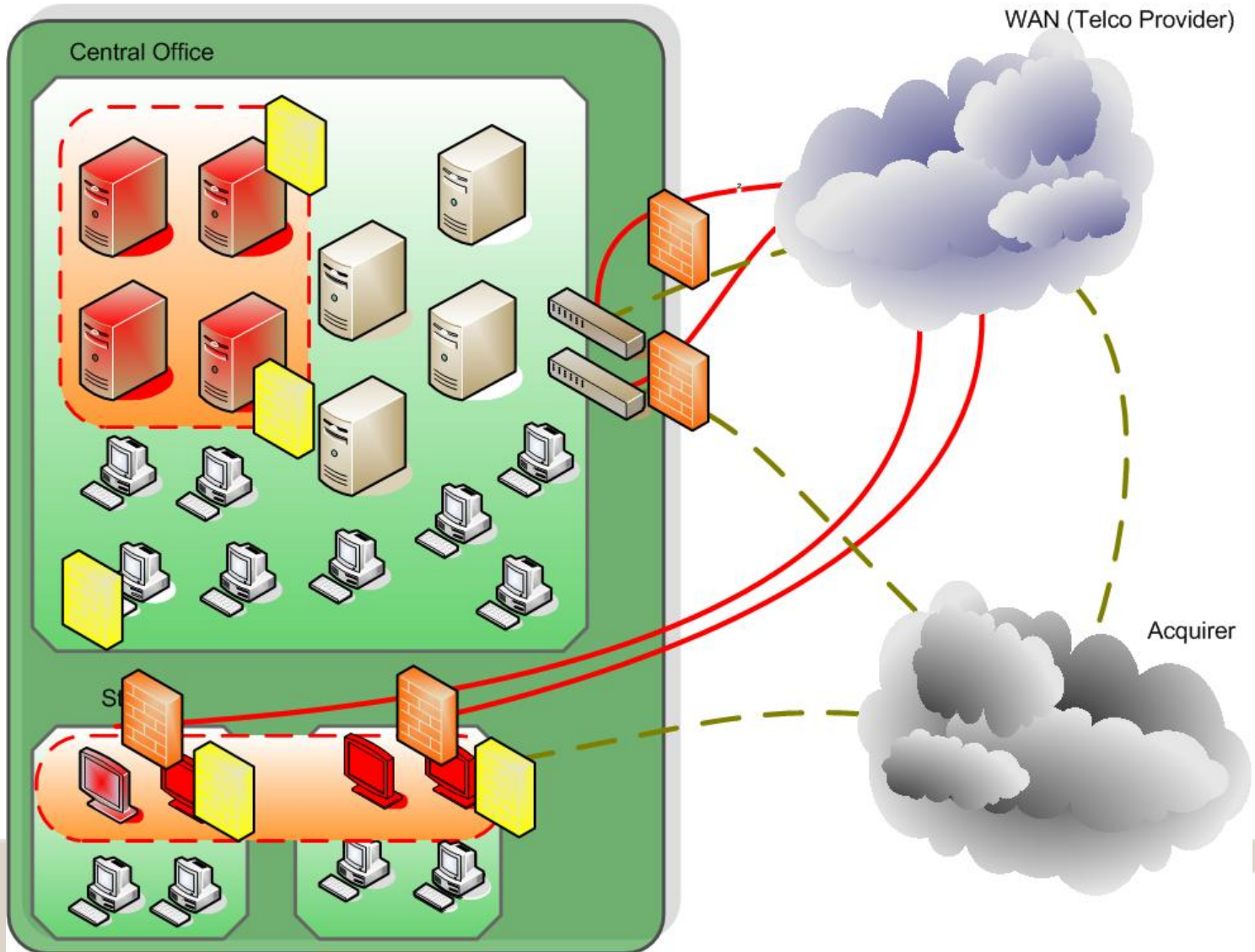
PCI-DSS is here!

Add layers of defense



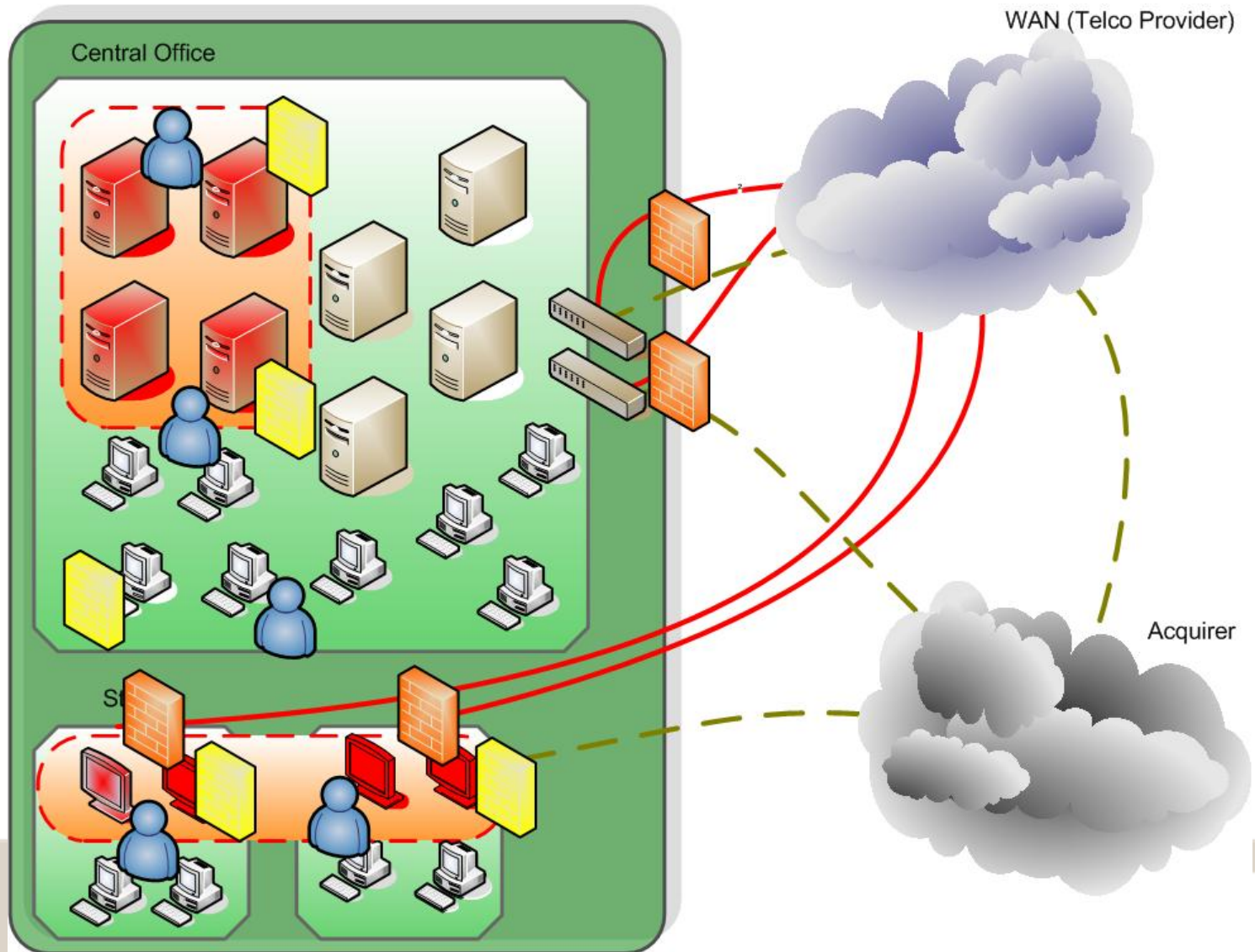
PCI-DSS is here!

Add other layers of defense



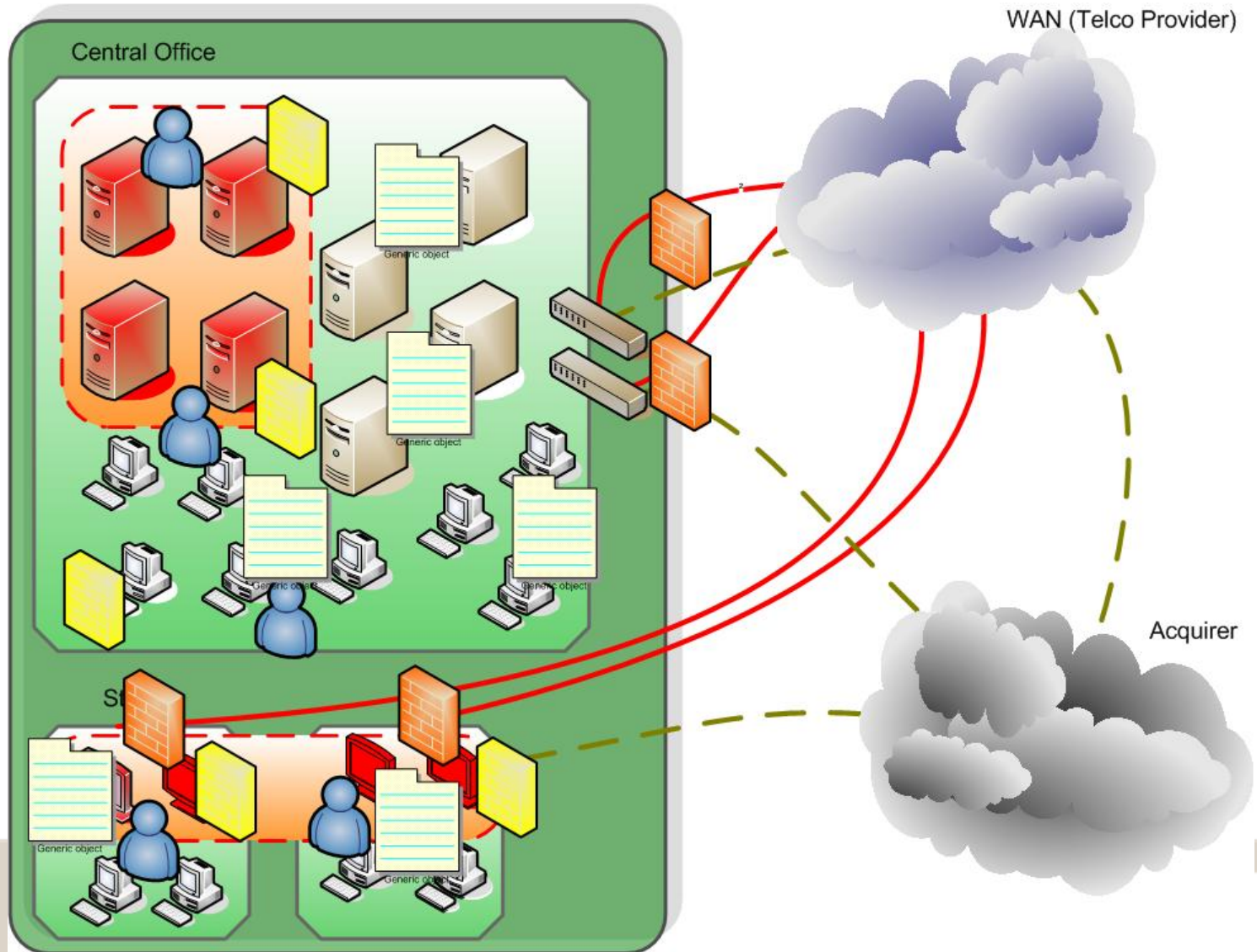
PCI-DSS is here!

Put people in place to check



PCI-DSS is here!

Policies and procedures



Risk options regarding PCI-DSS (or any other compliance)

- Risk Avoidance
- Risk Reduction/mitigation
- Risk Sharing
- Risk Transfer
- Risk Acceptance

Risk options regarding PCI-DSS (or any other compliance)

- ~~Risk Avoidance~~
- Risk Reduction/mitigation
- Risk Sharing
- Risk Transfer
- Risk Acceptance

Risk options regarding PCI-DSS (or any other compliance)

- ~~Risk Avoidance~~

- Risk Reduction/mitigation

- Risk Sharing

- ~~Risk Transfer~~

- Risk Acceptance

Risk options regarding PCI-DSS (or any other compliance)

- ~~Risk Avoidance~~

- Risk Reduction/mitigation

- Risk Sharing

- ~~Risk Transfer~~

- ~~Risk Retention~~

Risk options regarding PCI-DSS (or any other compliance)

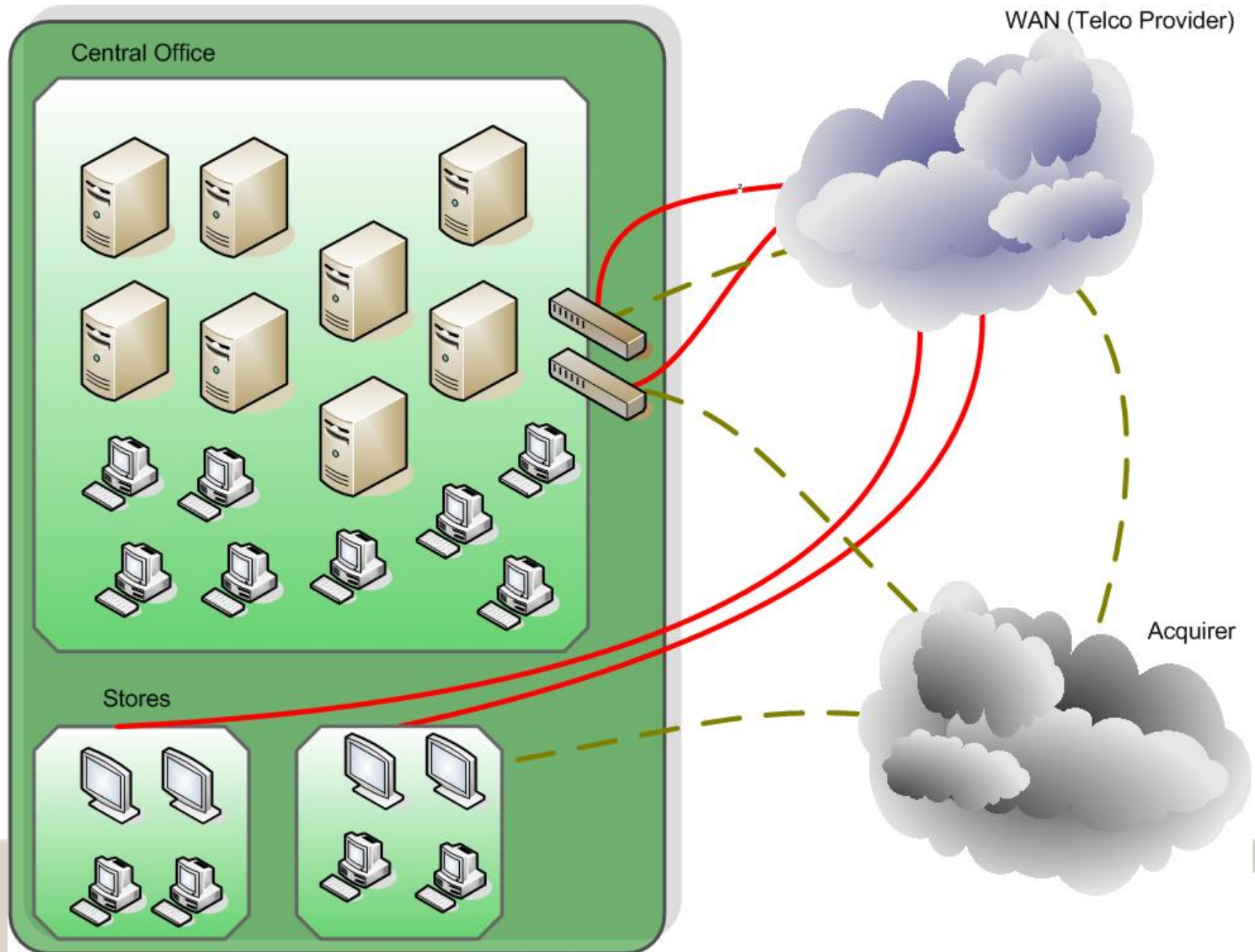
■ ~~Risk Avoidance~~

- Risk Reduction/mitigation
- Risk Sharing

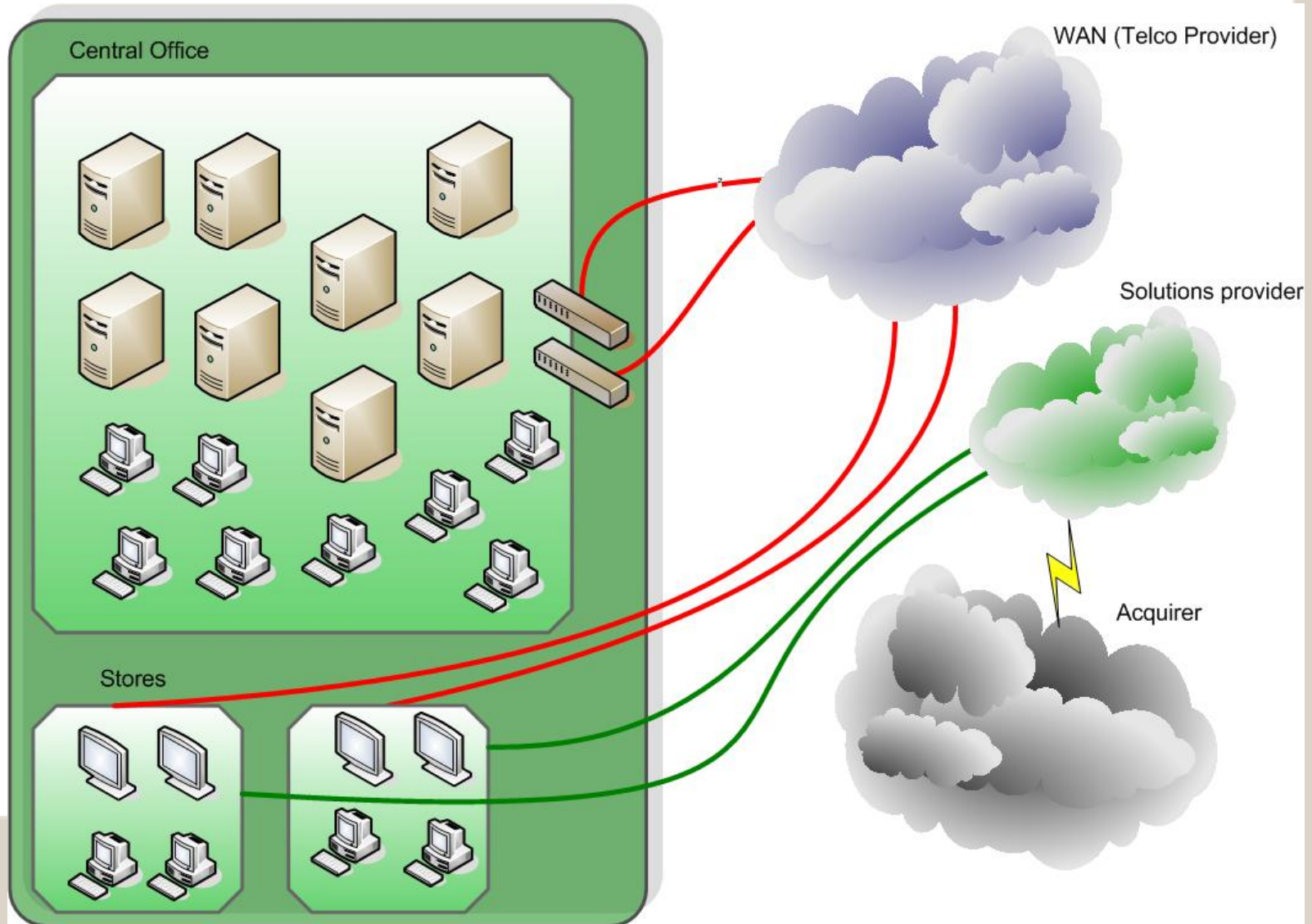
■ ~~Risk Acceptance~~

■ ~~Risk Transference~~

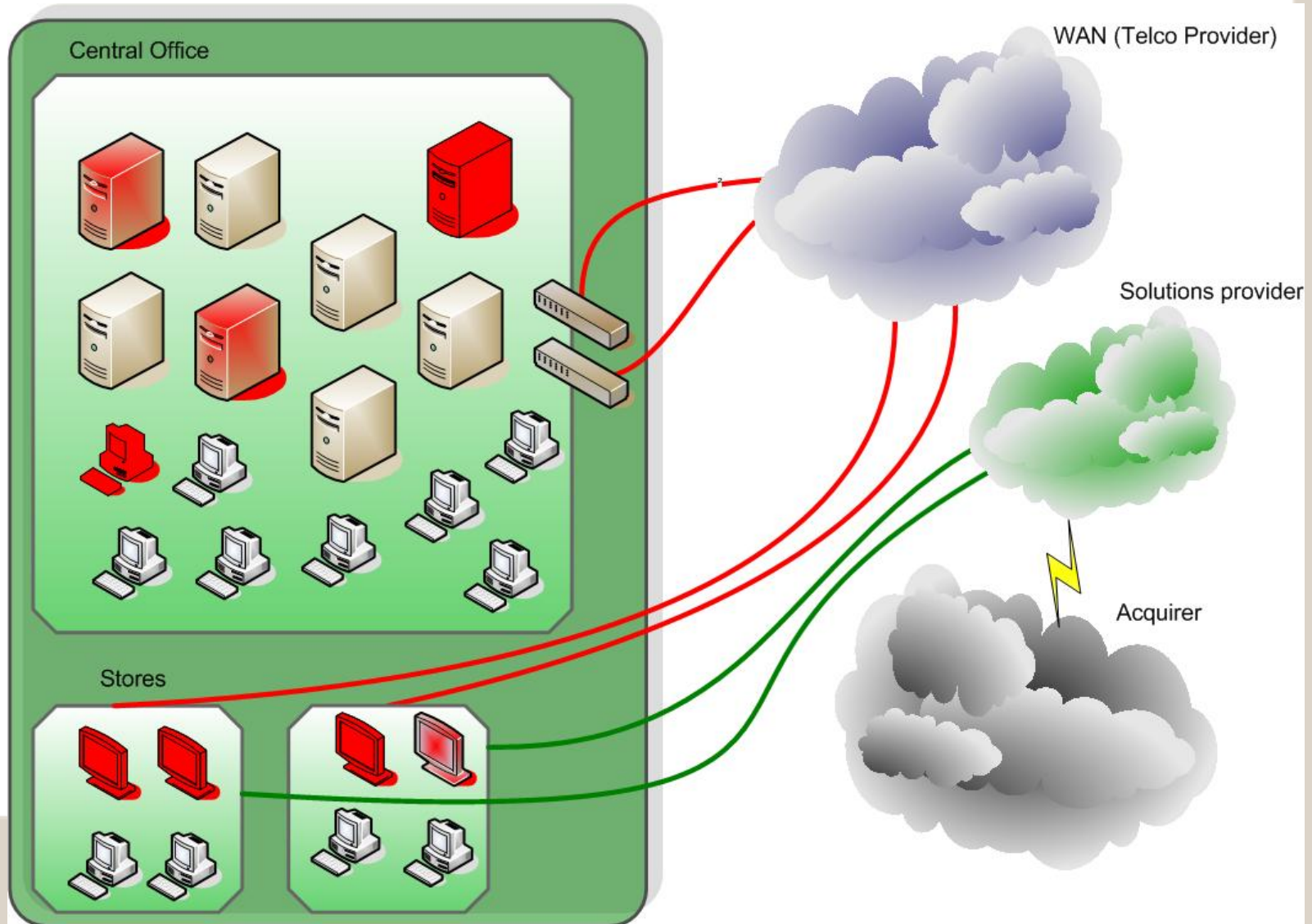
PCI-DSS outsourced



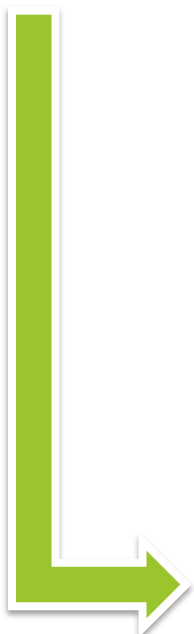
PCI-DSS outsourced – step 1



PCI-DSS outsourced – step 2



PCI-DSS outsourced process

- 
- Discuss with business
 - Don't change the “what”, but the “how”
 - Eliminate where possible
 - Get buy-in
 - Discuss with IT
 - Match the business discussion with IT

Define the level of outsourcing

- Get a solid contract
 - The provider MUST be PCI-DSS compliant
- Outsourcing = NOT elimination

PCI-DSS does not disappear

- Create and maintain policies, standards and procedures
- Take care of historical data
- Management and monitoring of PCI-DSS related infrastructure remains
- Double check for business (CHD) processes

(And you're done...)

Agenda

What is PCI-DSS?



PCI-DSS version 2.0



AB Vassilopoulos Case

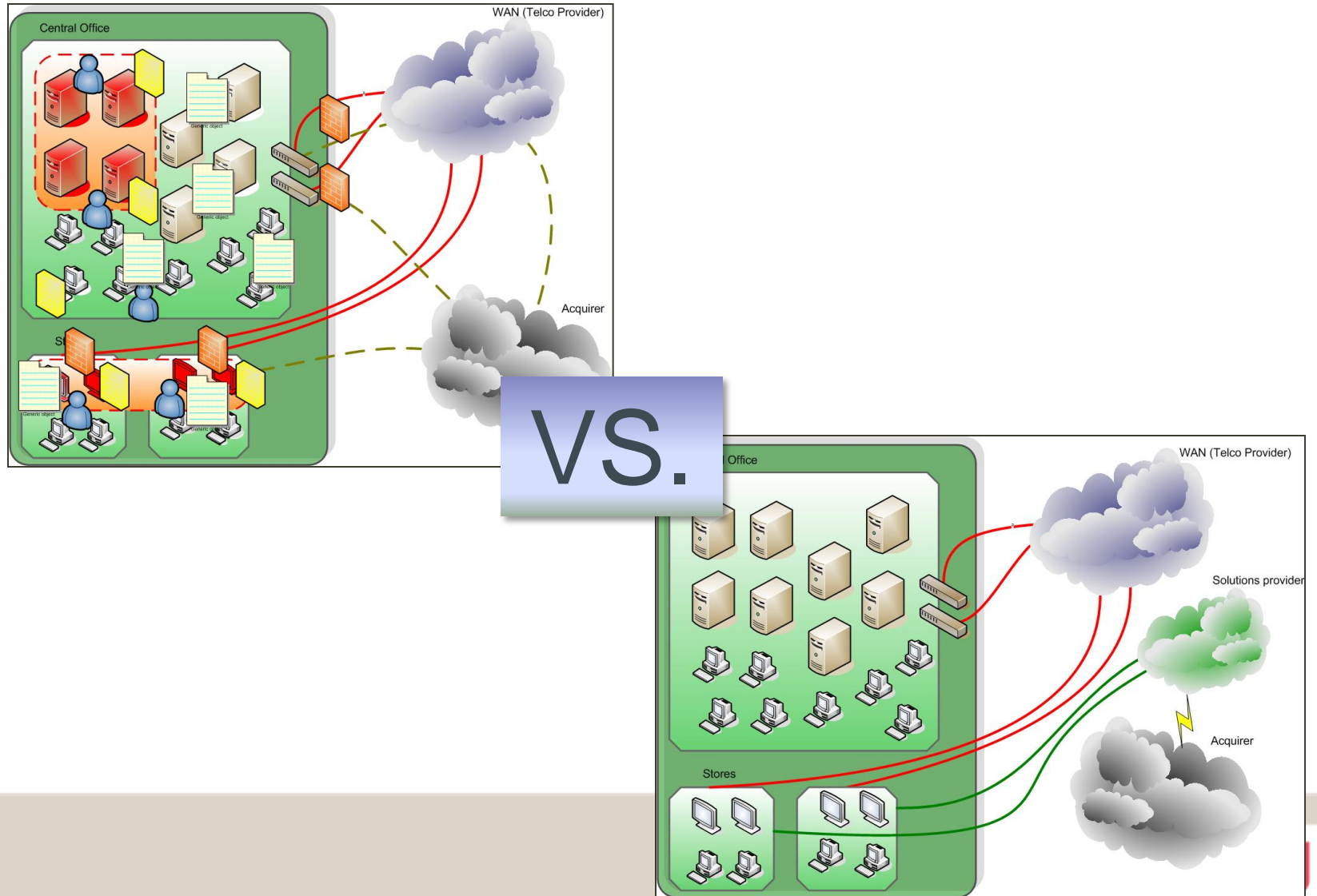


Costs and conclusion



Q&A

What does it cost?



What does it (still) cost?

- Cost accounts:
 - Human resources
 - Project management
 - Documentation
 - Business process changes
 - Contract costs
- End total: almost equal cost

Why then outsource?

- Sharing of risk
 - (PCI-DSS is all about risk *transfer*)
- Offloading of invisible costs
- Avoid cost of “non compliancy”
- Avoid cost of “data breach”
 - 204 \$ / record breached*
 - Average 6,75 million \$ / breach*
- Not the core business

Conclusion

- Make it a business project
- Clearly define level of outsourcing
- Realize it will still cost €€€

Make it work for you,
not against you.

determination | integrity | courage | humility | humor

THANK YOU

○ Outsourcing PCI-DSS

perceptions, fictions, and realities



Delhaize Group
David Callebaut, CISM
Information Security Officer
+32 2 412 82 09
dcallebaut@delhaize.be



Trust in, and value from, information systems

Belgium Chapter