

RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CIN-W04

Maximizing Security and Compliance through Digital Third Party Risk Management



#RSAC



Connect **to**
Protect


Leonel Navarro
PMP, CISM, CISSP, ISO27001LA

Global Information Security Practice
Director
@SofttekSecurity

Back in 1962



https://en.wikipedia.org/wiki/The_Jetsons

- 
- Agenda
 - 3rd party risk management: the challenge
 - The state of digital 3rd party risk 2016: Insights
 - Takeaways

Two Worlds Convergence



Physical

- Raw Materials
- Logistics
- Storage
- Warehouses
- Distribution Centers



Logical

- Applications
- Networks
- RFID / WiFi
- Information Exchange
- PII / Healthcare
- Banking
- Logistics

[illegible]

**You are using systems in every direction,
seeking to automate work to achieve
company goals...**

Like it or not, you have little choice
other than to trust others with your
information, and rely on their
services and systems

**How many 3rd Parties do you
integrate into your business?**



Cost and reputation damage explosion




- “19% of organizations suffered reputational damage as a result of a 3rd party supplier” - Forbes Insights Fallout: The Reputational Impact of IT Risk.
- “49% of companies have experienced a data breach through one of their vendors” - Data Risk in the Third Party Ecosystem, Ponemon Institute, April 2016.
- “65% of companies experienced a supply chain disruption due to cyber-attacks” - IT Disruption Risk, APQC, April 2015.

Cost and reputation damage explosion



- “More than half of organizations suffer damage to at least 20% of its value” - 2016 Cost of Data Breach Study: Global Analysis, Ponemon, June 2016.
- “\$221 cost per record lost (US).” - 2016 Cost of Data Breach Study: Global Analysis, Ponemon, June 2016.
- “28% of the supply chain disruptions lead to reporting balance sheet impacts” - Supply Chain Risk Management Study, Supply Chain Insights LLC, July 2015.

**What do you think is the % of
data breaches associated to 3rd
Parties?**



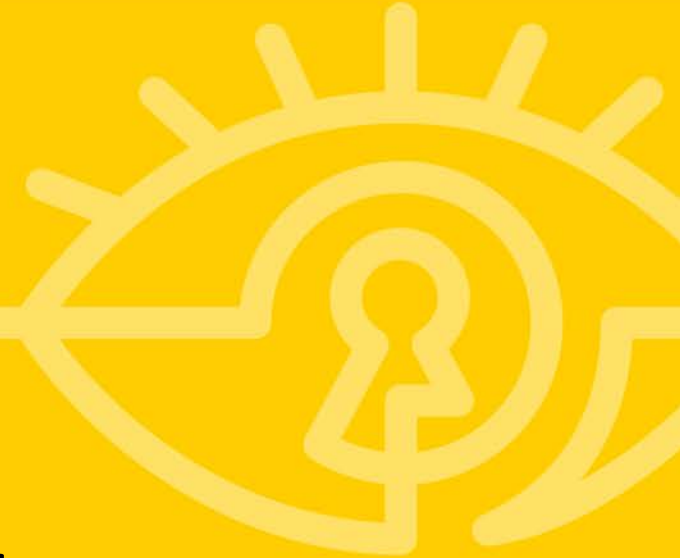
Source of data breaches



The State of Digital Third-Party Risk 2016 Report - <http://en.softtek.co/tprisk2016>

**Digital 3rd Party Risk Management is
the bridge to do so properly and
securely.**

**Which of your vendors
represent the highest risk to
your organization?**



Digital Third-Party Risk Management



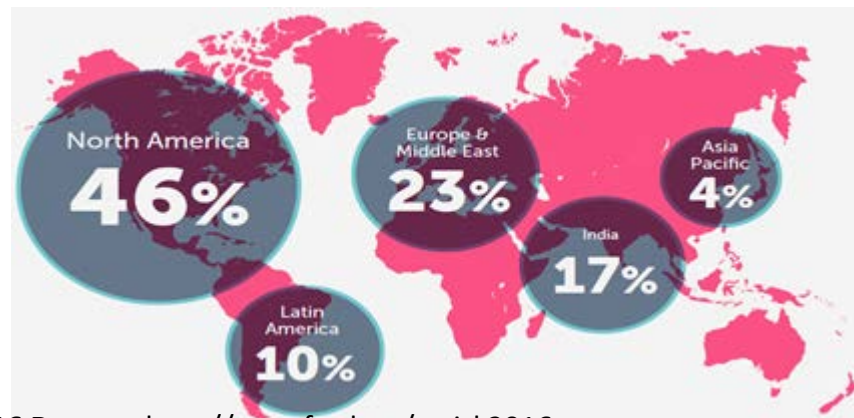
- Third-party risk profiling
- Risk-based assessment
- Effective due diligence
- Support in remediation
- Continuous process & metrics based



The state of Digital Third-Party Risk Report 2016



- 1,236 Security & Risk Assessments from 2014 and 2015
- 286 Controls aligned to ISO 27001
- 14 Security Domains



Top 10 Security controls that third parties fail on initial assessment



Rank	Control	Security Domain	Suppliers Failing Control
1	Secure disposal or reuse of equipment	Physical and Environmental Security	52.8%
2	Information systems audit controls	Operations Security	50.6%
3	Policy on the use of cryptographic controls	Cryptography	49.5%
4	Management of technical vulnerabilities	Operations Security	46.1%
5	Removal or adjustment of access rights	Access Controls	32.9%
6	User access provisioning	Access Controls	26.4%
7	Unattended user equipment	Access Controls	26.3%
8	Screening	Human Resource Security	24.8%
9	Network controls	Network Security Management	24.6%
10	Policies for information security	Information Security Policies	22.2%

3rd Party Security Domain Risk Quadrant



Best-in-class and worst-in-class benchmarks

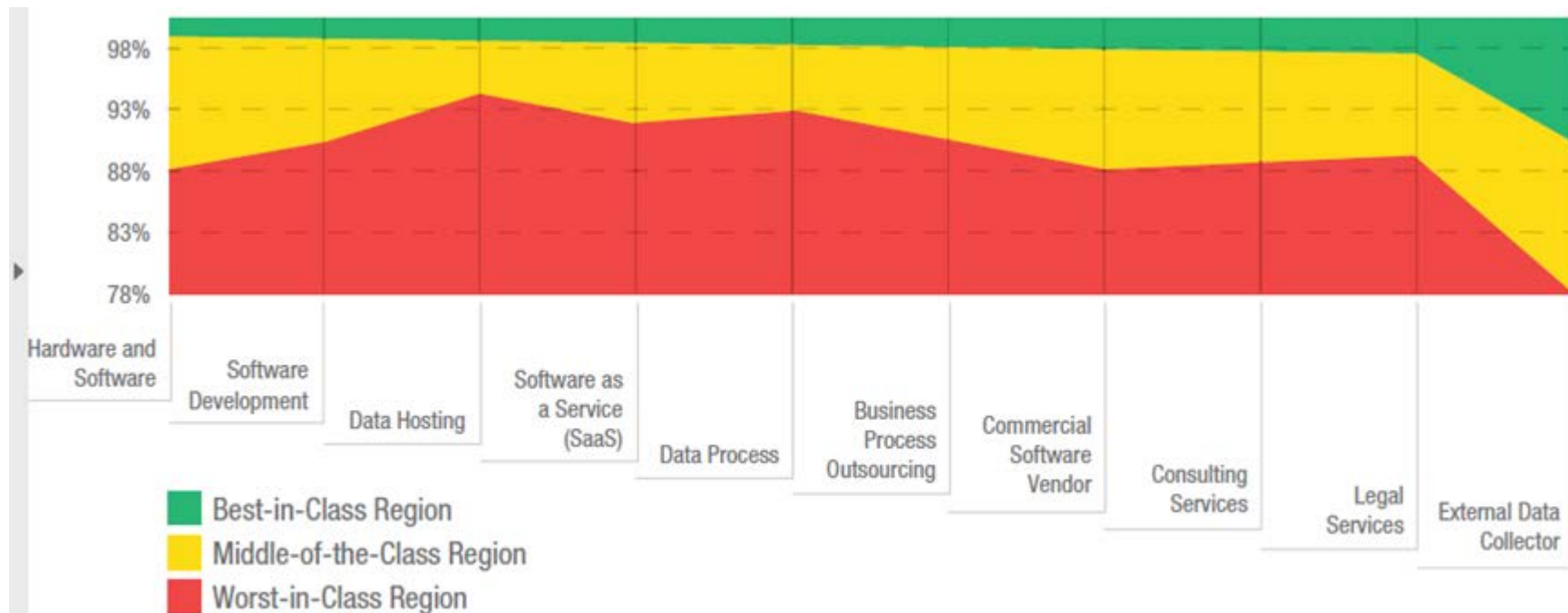
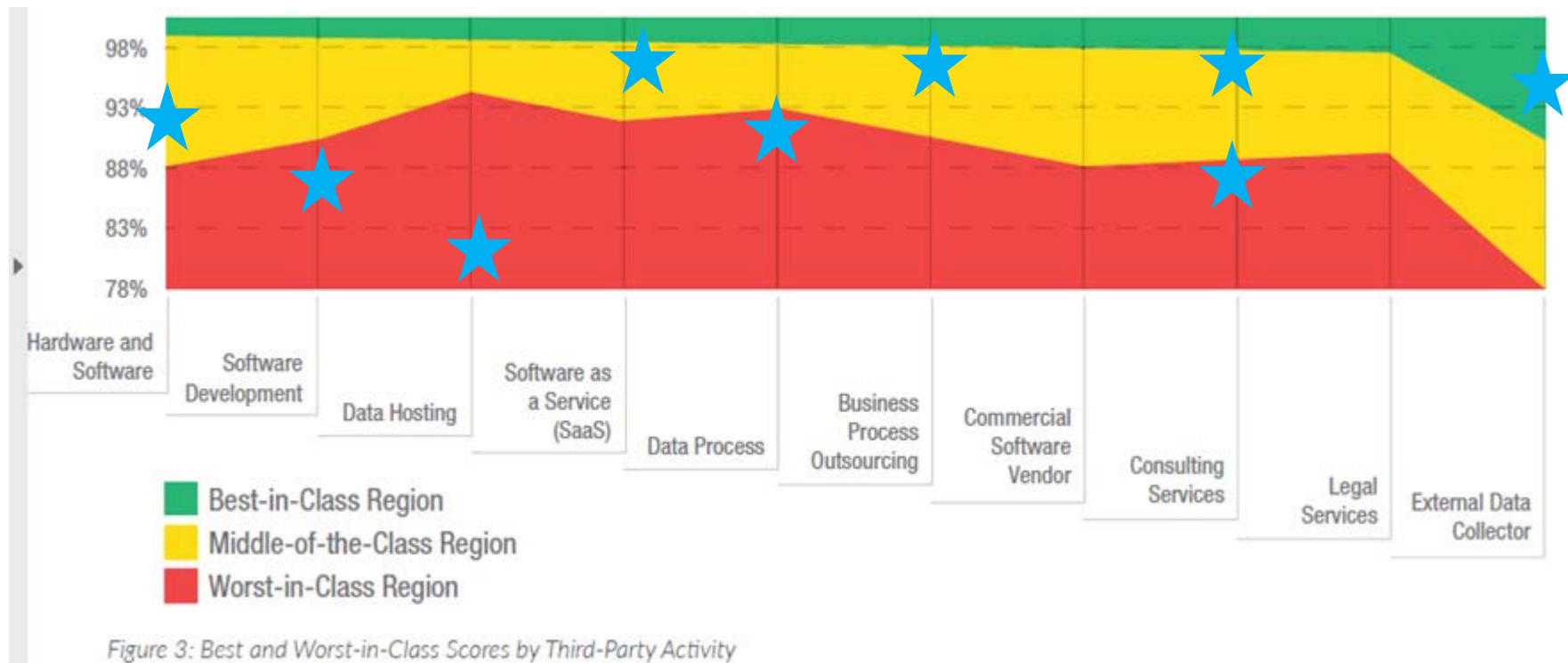


Figure 3: Best and Worst-in-Class Scores by Third-Party Activity

Best-in-class and worst-in-class benchmarks



Best-in-class and worst-in-class benchmarks

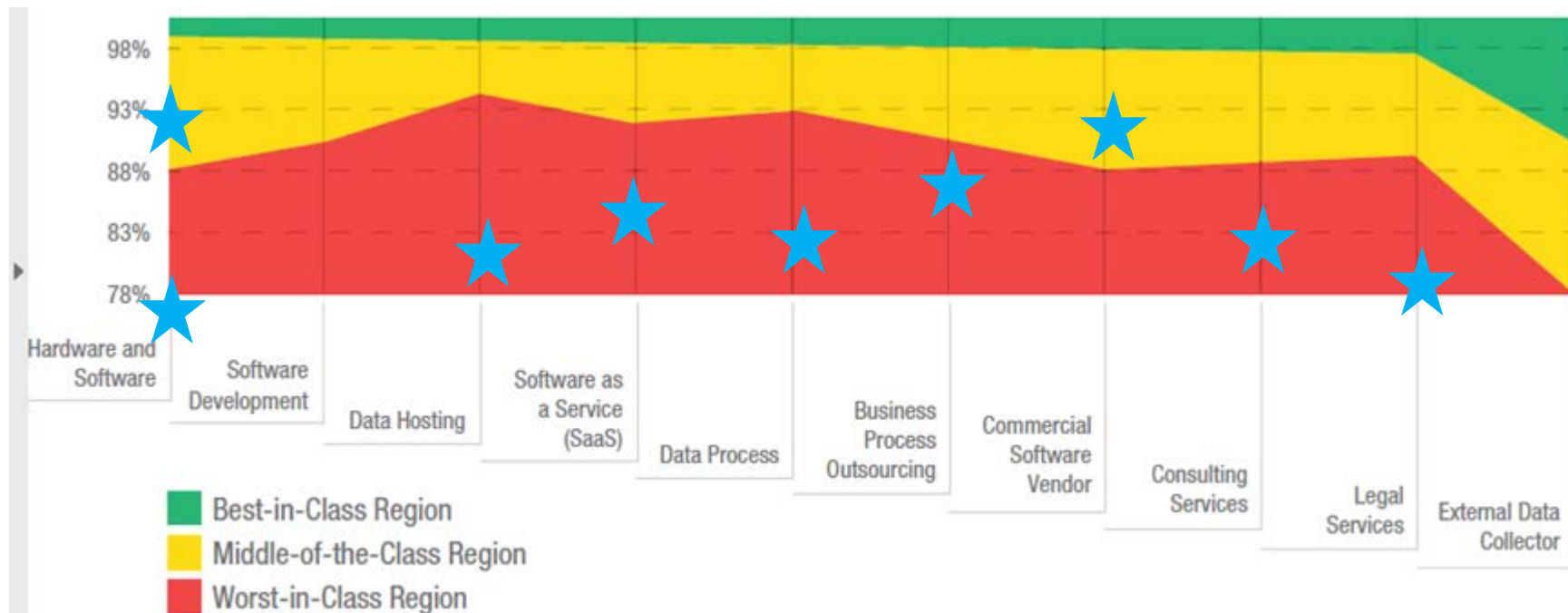


Figure 3: Best and Worst-in-Class Scores by Third-Party Activity

**Where would your third-parties
rank against Best-in-class
benchmarks?**



Scoring your third-parties



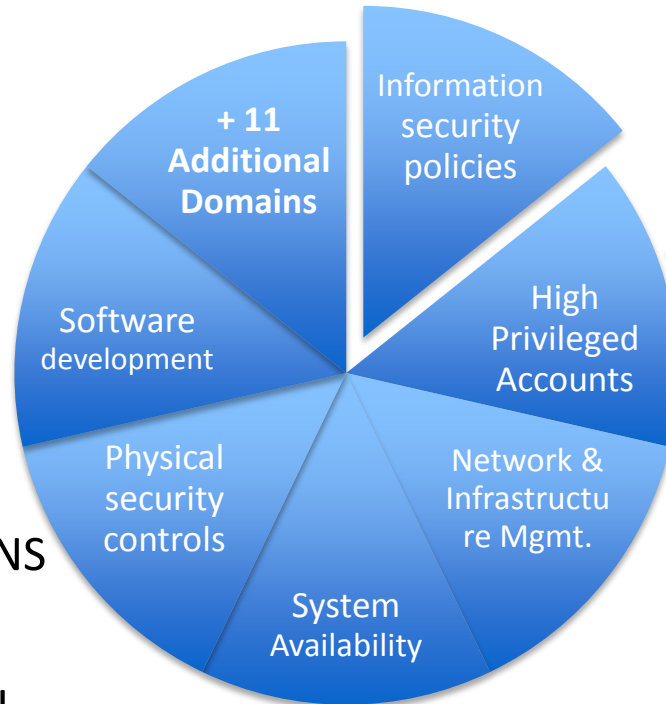
Risk Level	Data Sensitivity	Data Usage	Service Location
3: High	Confidential Information	Processing	Remote with direct connection (VPN, P2P, B2B VPN)
2: Medium	Private Information	Reporting / Consulting	Remote without direct connection (email, ftp, uploads, downloads)
1: Low	Public Information	Storage	Onsite

- Classify 3rd parties based on risk profiles
- Identify risks and classify them based on likelihood and impact
 - Likelihood : Occurrence percentage
 - Impact: Integrity, Confidentiality Availability
 - Other factors:
 - Regulatory or contractual requirements
 - Sensitivity or criticality of data assets

Scoring your third-parties



- Personalized
 - Risk Profile
 - Industry
 - 3rd-party
- Aligned
 - ISO 27001 or SANS 20CSC
 - SSAE16, SOX, PCI



- Organization of information security
- Human Resource Mgmt.
- HR Security and Procedures
- Communication & Operations Mgmt.
- Access Control
- Incident Management
- Data Security and Change Mgmt.

Delivery of the questionnaire:

- Sending questionnaires in Excel format (encrypted)
- Online portals to share and upload documents
- Specific tools for assessment

Scoring your third-parties



**Level 1 :
Excellent**

Complies with ALL controls audited

**Level 2:
Good**

Meets all Critical and High risk controls but fails on Low level controls.

**Level 3:
Acceptable**

Meets only critical controls, but fails on High and Low controls.

**Level 4:
Weak**

Does not meet critical controls and is pending remediation for high and low controls.

**Level 5:
Poor**

Does not meet any critical and high controls.



Digital 3rd Party Risk Management Framework



Management – Reporting – Support

3rd Party Audit Management

3rd Party
Inventory

3rd Party
Profiling

Risk
Assessment

Evidence
Gathering

Report
Generation

3rd Party
Mitigation Plan

Metrics

Generation

Analysis

Action plan
definition

Policies & Standards

3rd Party Policy
Definition

Contractual
Guidelines

Training
& Awareness

Remediation Support & Follow up

Remediation
Support

Evidence
Gathering

Verification

Process Improvement



Scoring your 3rd parties – frequent challenges



Questionnaires

- Inconsistency of responses or incomplete answers
- No valid supporting documentation
- Key staff is not involved in the review process
- Failure to deliver requirements on time

Interviews

- Lack of confidence in controls not supported with valid evidence
Processes are not defined or documented
- Lack of commitment to perform checkpoints



3rd Party Risk Management – Banking Case Study



At a Glance

- › Business : Banking and Finance
+35,000 employees in 40 countries
- › Target Third Parties: +180

Challenges

- › Reduce 3rd party overall risk
- › Engage with sponsor/3rd-party contacts to agree upon remediation plans.
- › Empower sponsors to take decisions about 3rd-party' security controls.
- › Track 3rd-party' security assessments progress performed every 2 years.
- › Analyze 3rd-party's findings to implement proactive controls.



The Solution

- Establish a 3rd party risk & security audit program:
- › Provide a standard process to schedule, execute and track security audits.
- › Assign and implement action items that lead to the findings' resolutions.
- › Provide the necessary metrics to report risk levels to upper management and ease decision taking.

Voice of the Customer

“The 3rd Party security audit program has standardized and improved the effectiveness of closing assessment findings. This process' consistency and follow up has significantly reduced 3rd Party risk.”

Third Party Information Security Leader
Top 20 Banking Organization

3rd Party Risk Management Benefits



- Appropriate vendor alignment to company goals/policies over the time
- Risk mitigation thru right treatment
- Documented risk exposure
- Continuous follow up & continuous improvement
- Proactive risk identification
- Risk remediation strategy per supplier
- Cost effective solution for vendors risk mitigation
- Happy CEO / CIO / CRO

Apply What You Have Learned Today



Short Term
1 - 2 months

- Implement Life Cycle Vendor Risk Management.
- Provide feedback to vendors on findings & enforce protection & compliance.
- Generate metrics and define a continuous process improvement plan.



Mid Term
2 to 6 months

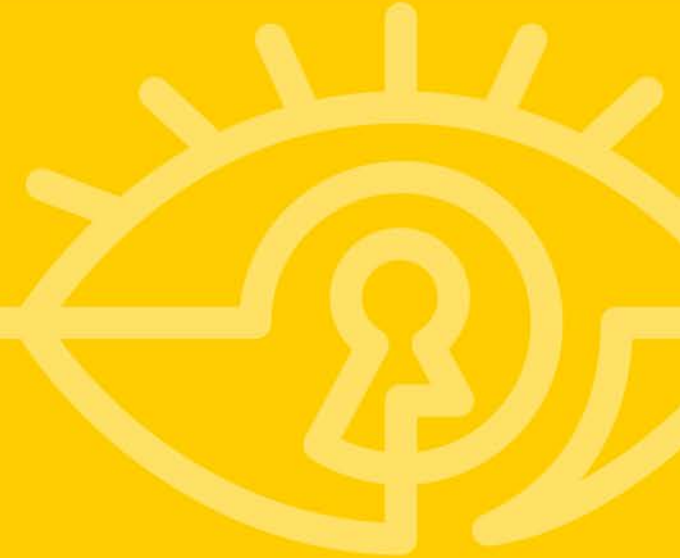
- Require supplier evidence that shows efficacy in incident response process.
- Maintain inventory of suppliers, including criticalities to core processes.
- Manage the vendor risk profiles.



Long Term
6 months to 1+ year

- Review & adhere to the Internal Procurement Process (VMO, CRO).
- Assess new suppliers to measure the level of cyber security compliance (CISO, CRO).
- Improve supplier contractual terms to include vital security requirements.
- (CRO, CISO, VMO).

Q&A



Leonel Navarro, PMP,CISSP,CISM,ISO27001LA

leonel.navarro@softtek.com

@SofttekSecurity @LeonelNavarroS