RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: STR-W02

The state of digital supplier risk management: In partners we trust

Leonel Navarro, PMP, CISSP, CISM, ISO27001LA
Global Information Security Practice Director
Softtek
@SofttekSecurity

RSAConference2017

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.

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

RSAConference2017

How many third parties do you think an organization integrates into its business?

Cost and reputation damage explosion

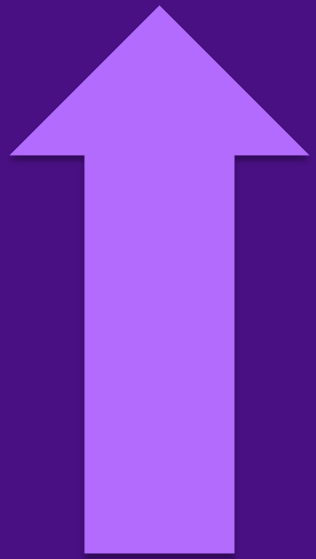
- "49% of companies have experienced a data breach through one of their vendors" - Data risk in the third party ecosystem, Ponemon Institute, April 2016.
- "65% of companies experienced a supply chain disruption as a consequence of a cyber-attack" - IT Disruption risk, APQC, April 2015.
- "More than half of organizations suffer damage of at least 20% of their value" - 2016 Cost of data breach study: Global Analysis, Ponemon, June 2016.
- "28% of supply chain disruptions lead to reporting balance sheet impacts" - Supply Chain Risk Management Study, Supply Chain Insights LLC, July 2015.

RSAConference2017

What do you estimate to be the % of data breaches associated with third parties?

Source of data breaches

Most likely source of a data breach that results in misuse of confidential or sensitive information.



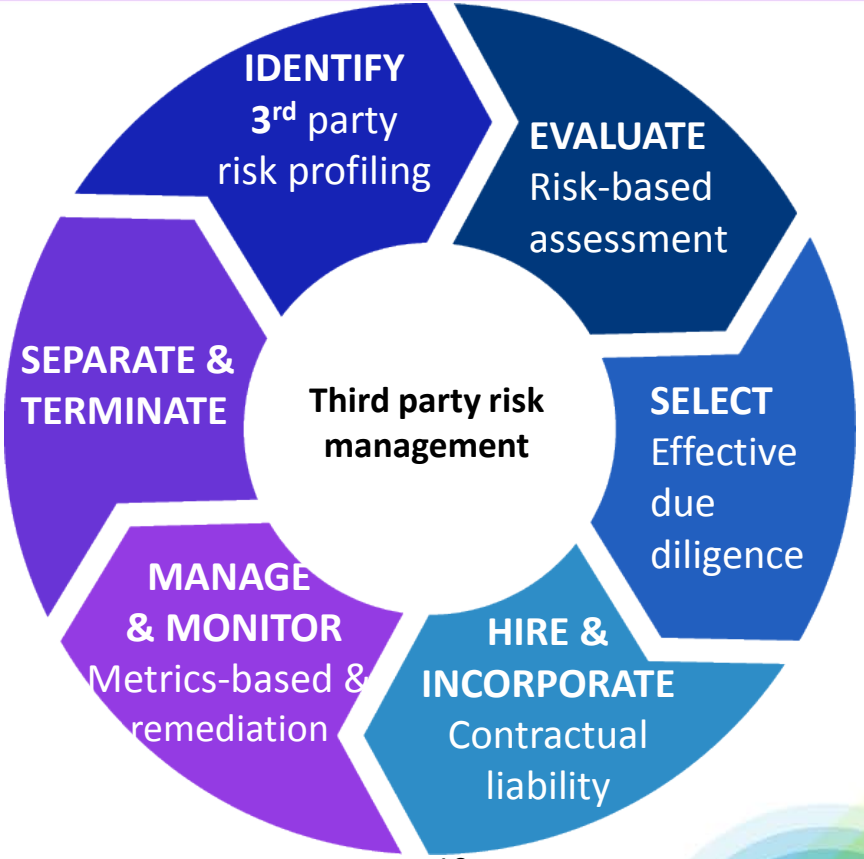
The State of Digital Third-Party Risk 2016 Report - http://en.softtek.co/tprisk2016

Which one of your vendors poses the highest risk to your organization?

RSAConference2017

Digital third party risk management is an important bridge to increase security.

Digital third party risk management



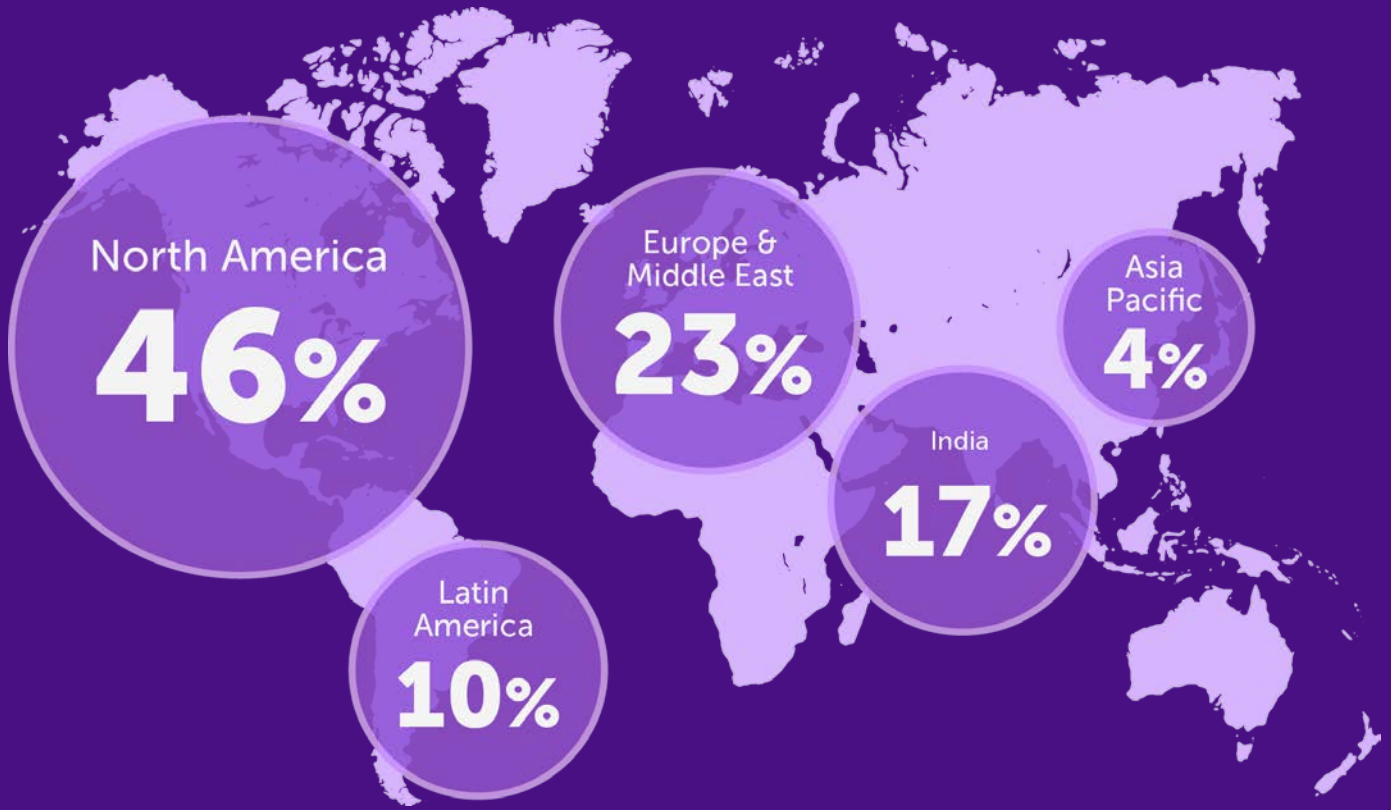
Softtek®

The state of digital third party risk 2016

- 1,236 Security & risk assessments
- 286 Controls aligned to ISO 27001
- 14 Security domains
- The State of Digital Third-Party Risk 2016 Report - http://en.softtek.co/tprisk2016

Softtek®

The state of digital third party risk 2016



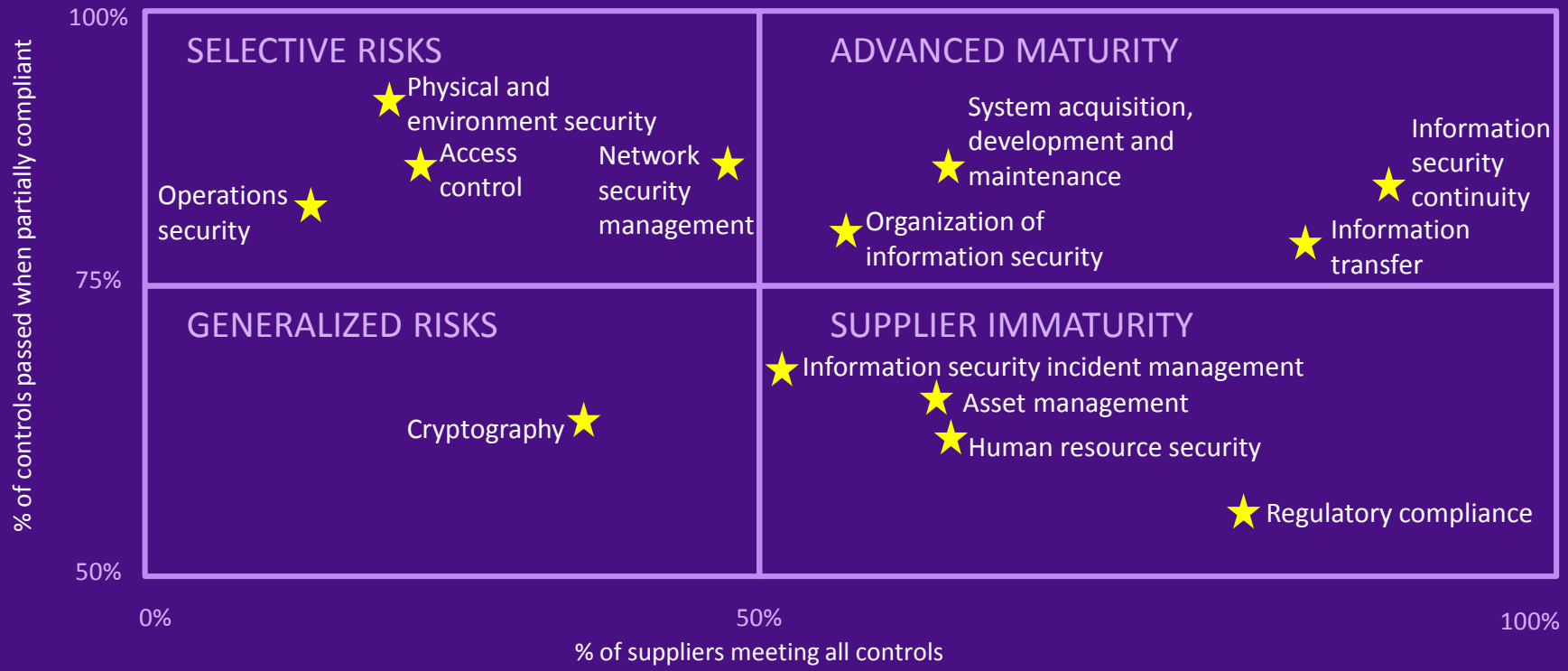
Top 10 security controls that third parties fail on initial assessment

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%

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

Softtek®

The state of digital third party risk 2016



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

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

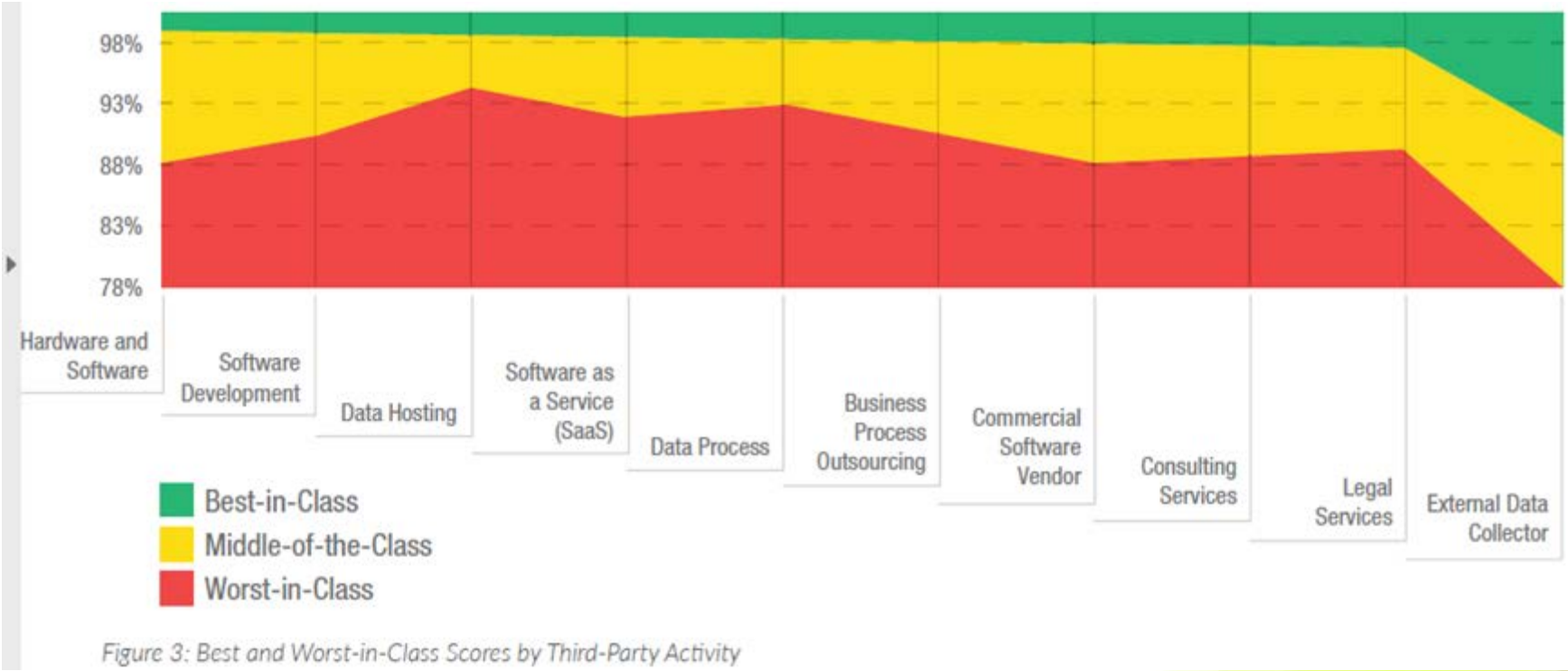


Figure 3: Best and Worst-in-Class Scores by Third-Party Activity

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

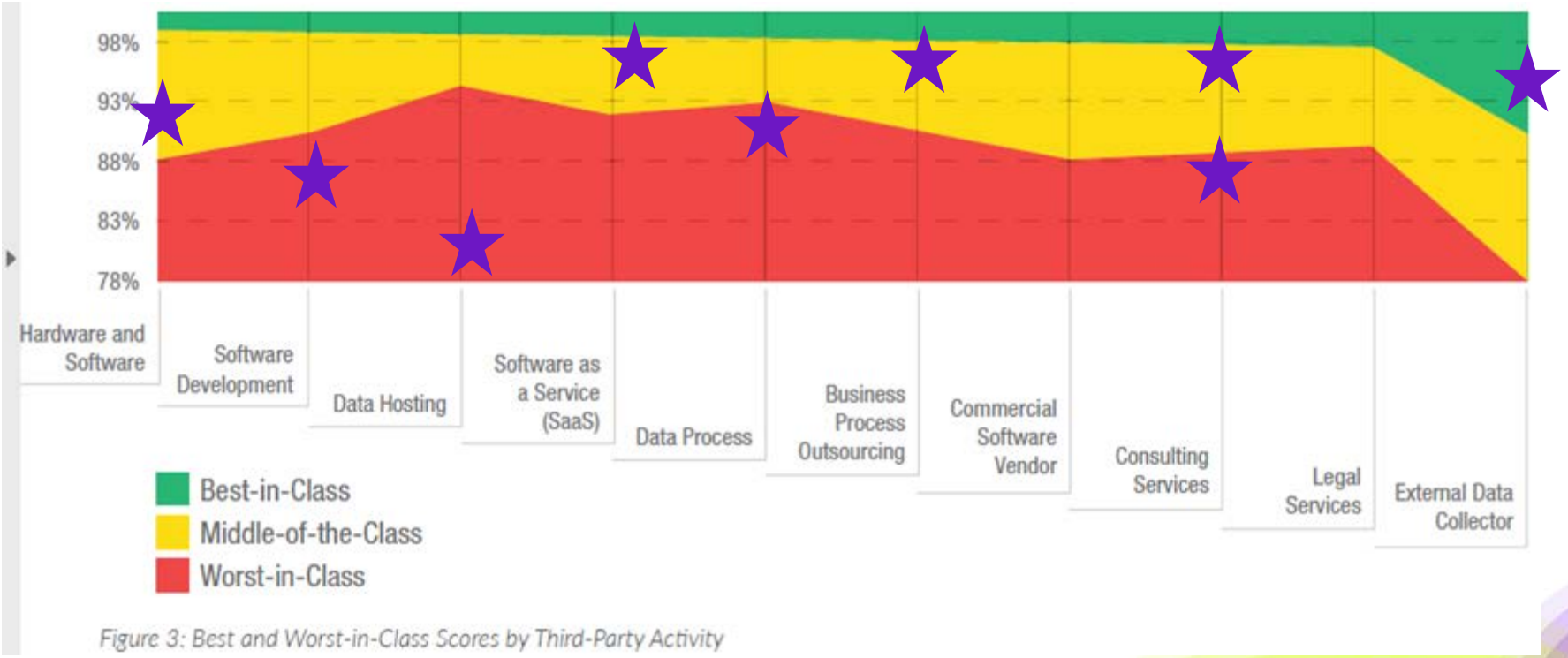


Figure 3: Best and Worst-in-Class Scores by Third-Party Activity

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

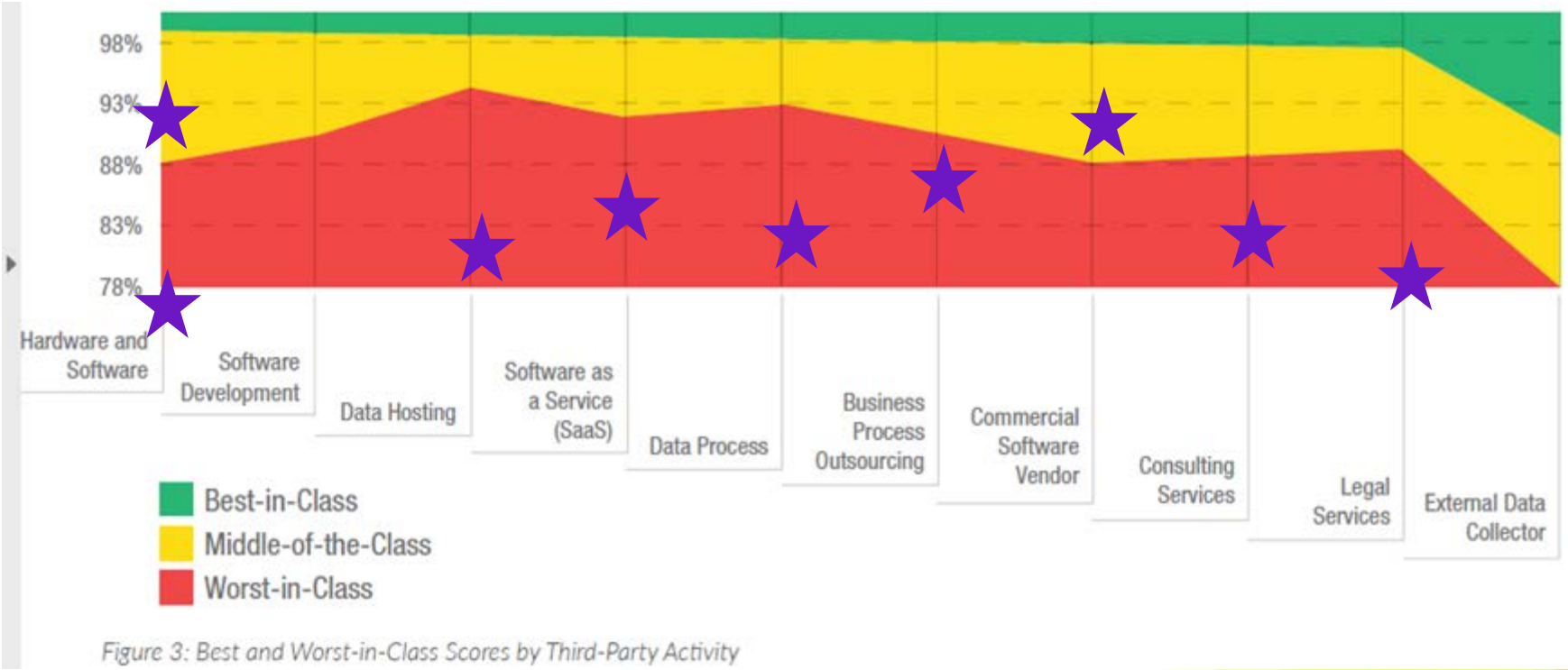


Figure 3: Best and Worst-in-Class Scores by Third-Party Activity

RSAConference2017

How would your third parties rank against best-in-class benchmarks?

Scoring your third parties

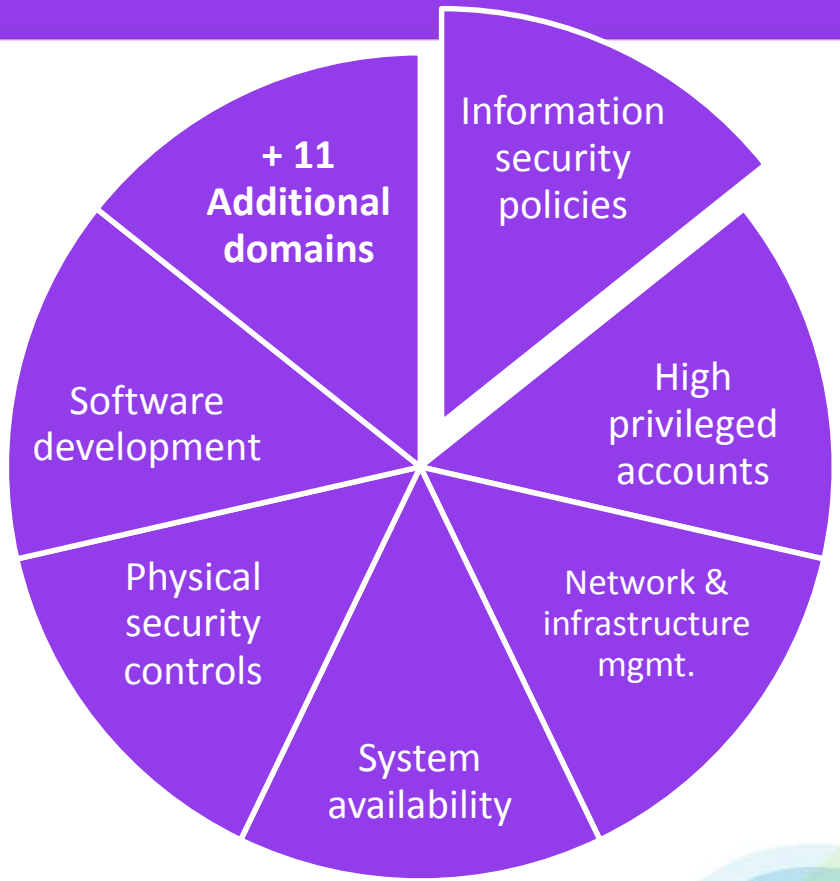
Risk Level	Data Sensitivity	Data Usage	Service Location
3: High	Confidential Information	Processing	Remote with direct connection (VPN, P2P, B2B VPN)
2: Medium	Private Information	Reporting / Consulting	Remote without direct connection (email, ftp, uploads, downloads)
1: Low	Public Information	Storage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

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

Softtek®

Scoring your third parties

- Customized
  - Risk profile
  - Industry aligned
  - 3rd party category
- Aligned
  - ISO 27001 or SANS 20CSC
  - SSAE16, SOX, PCI



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

Softtek®

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 fail on high and low controls
Level 4: Weak	Does not meet critical controls and is pending remediation plan for high and low controls
Level 5: Poor	Does not meet any critical or high controls

Scoring your third parties

The state digital third party risk management framework

Management – Reporting – Support

Third party audit management

- Third party inventory
- Third party profiling
- Risk assessment
- Evidence gathering
- Report generation
- Third party mitigation plan

Metrics

- Generation
- Analysis
- Action plan definition

Policies & Standards

- Third party policy definition
- Contractual guidelines
- Training & awareness

Remediation Support & Follow-up

- Remediation support
- Evidence gathering
- Verification

Process Improvement

How do I apply this?

Apply what you have learned today

- Based on your risk profile identify your critical third parties
- Use the top 10 security controls list to open conversations
- Incorporate top 10 security controls to your next audit cycle
- Generate metrics, benchmark your third parties, and create internal awareness with them
- Incorporate security requirements (liability, fourth parties) into your contracts

Apply what you have learned today

- Follow the internal procurement process and evaluate the cyber risk from the beginning
- Perform due diligence with new third parties to understand their cybersecurity maturity level
- Define communication processes to deal effectively with security incidents
- Perform continuous process validation and verification
- Improve your lifecycle third party risk management program

RSAConference2017

Q&A

Leonel Navarro, PMP, CISSP, CISM, ISO27001LA
Softtek
@SofttekSecurity / @LeonelNavarroS