



# So You Think You Know Your SaaS Security Agreements?

Aparna Dasai Williams, NortonLifeLock  
John Bates, DocuSign  
Scott Plichta, CSC  
Helena Ledic, CSC



# Presenters



**Aparna Dasai Williams**

Senior Director  
NortonLifeLock Inc.  
[aparnaMDW@gmail.com](mailto:aparnaMDW@gmail.com)



**Helena M. Ledic**

Associate General Counsel  
CSC  
[helena.ledic@cscglobal.com](mailto:helena.ledic@cscglobal.com)



**John Bates**

Senior Counsel, Partner Ecosystem,  
CIPP/US  
DocuSign  
[john.bates@docusign.com](mailto:john.bates@docusign.com)



**Scott Plichta**

Chief Information Security Officer  
CSC  
[scott.plichta@cscglobal.com](mailto:scott.plichta@cscglobal.com)



# GDPR Breaches

Company Is Fined \$57 Million Under Europe's Data Privacy Law

Regulators Fine Company \$170 Million for Violating Children's Privacy Online

Hotel Faces Massive \$123 Million GDPR Fine For 2018 Security Breach

Department may face GDPR fine of up to €1m

Airline faces \$230M GDPR fine for 2018 data breach

Firm will have to work to rebuild trust after shock with GDPR fine

Watch Flags Possible Tech Company GDPR Breach





## Third-Party Breaches

Former cloud-provider employee  
created custom scanning software

30 companies breached with 20-30  
TB data downloaded

Analytics 3rd party vendor  
used Nth vendor

24 million records breached

Medical collections agency suffers  
breach on 13+M records

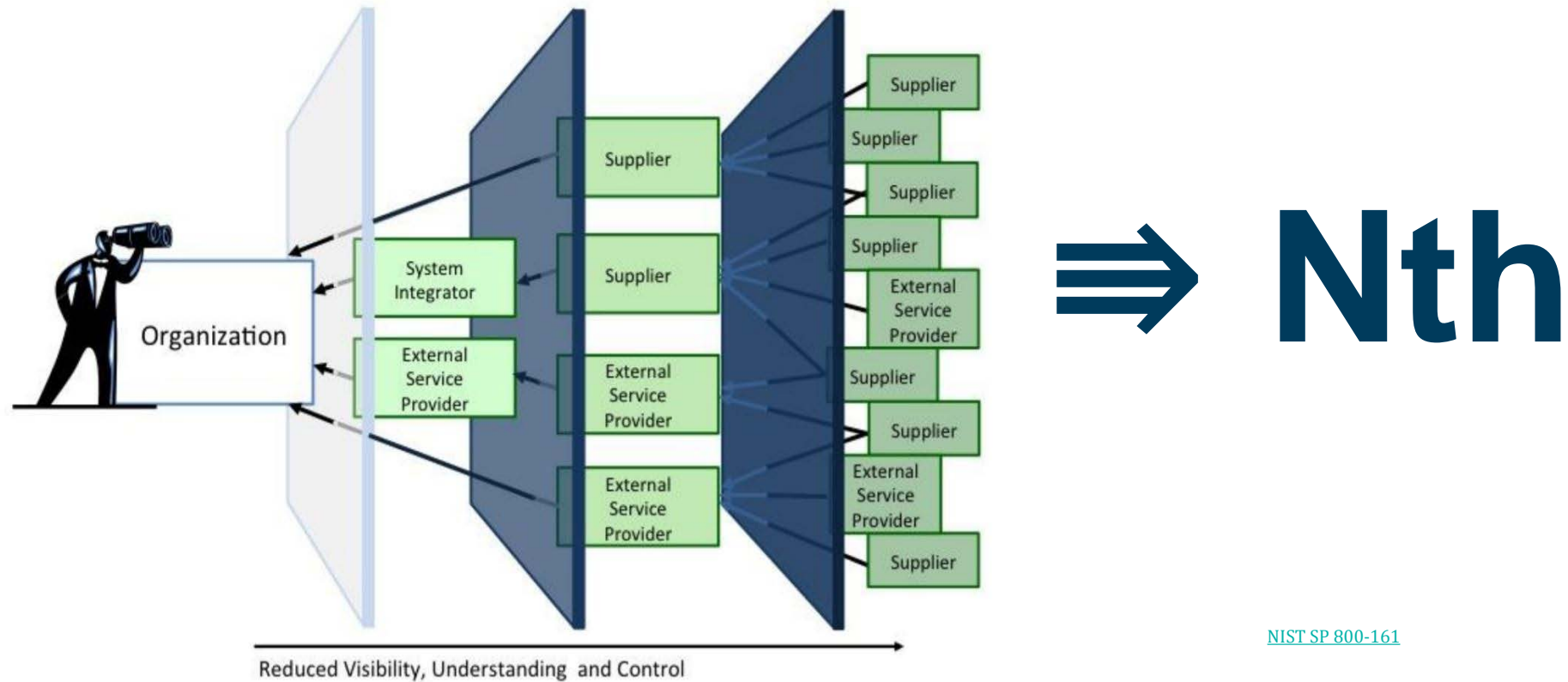
Loses 4 major clients

Files for Chapter 11

Fortune 500 conglomerate outsourced  
HR/payroll document processing functions  
to 3rd party who had data in an email account

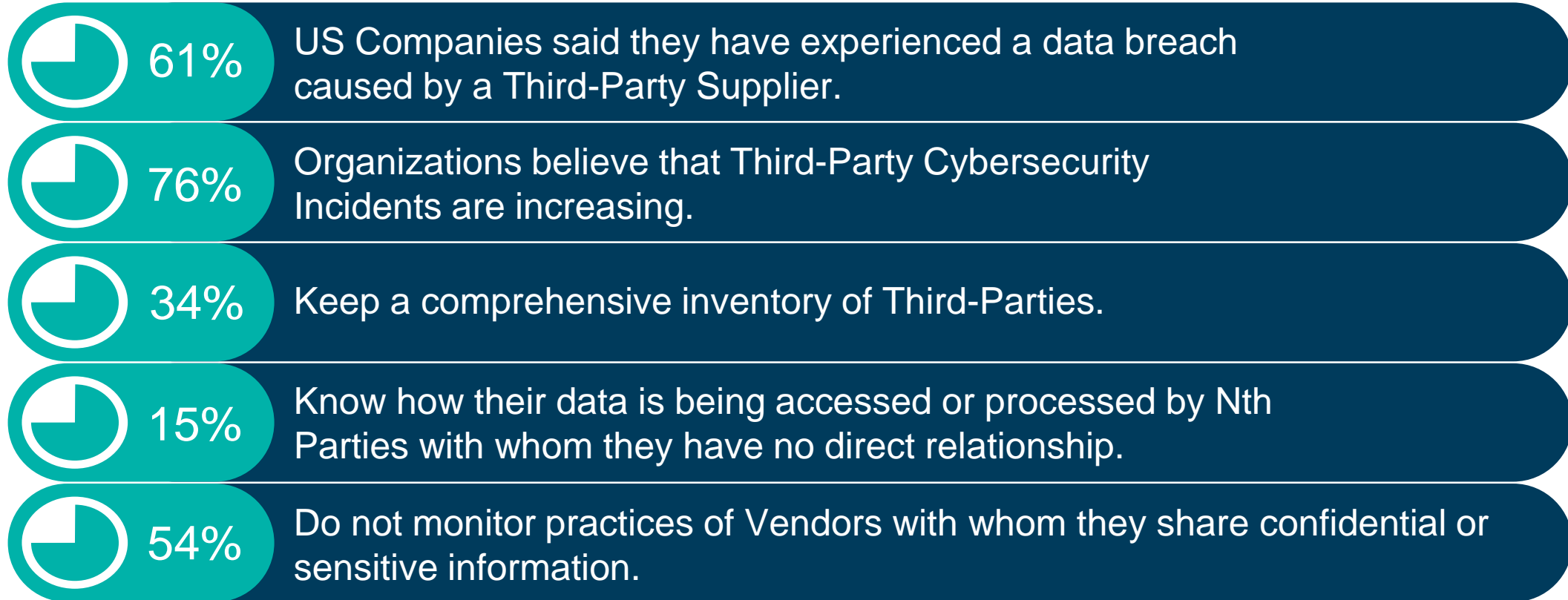
Employee SSNs, medical information,  
beneficiaries, passports, etc., disclosed

# Complexity Increasing with Nth Parties

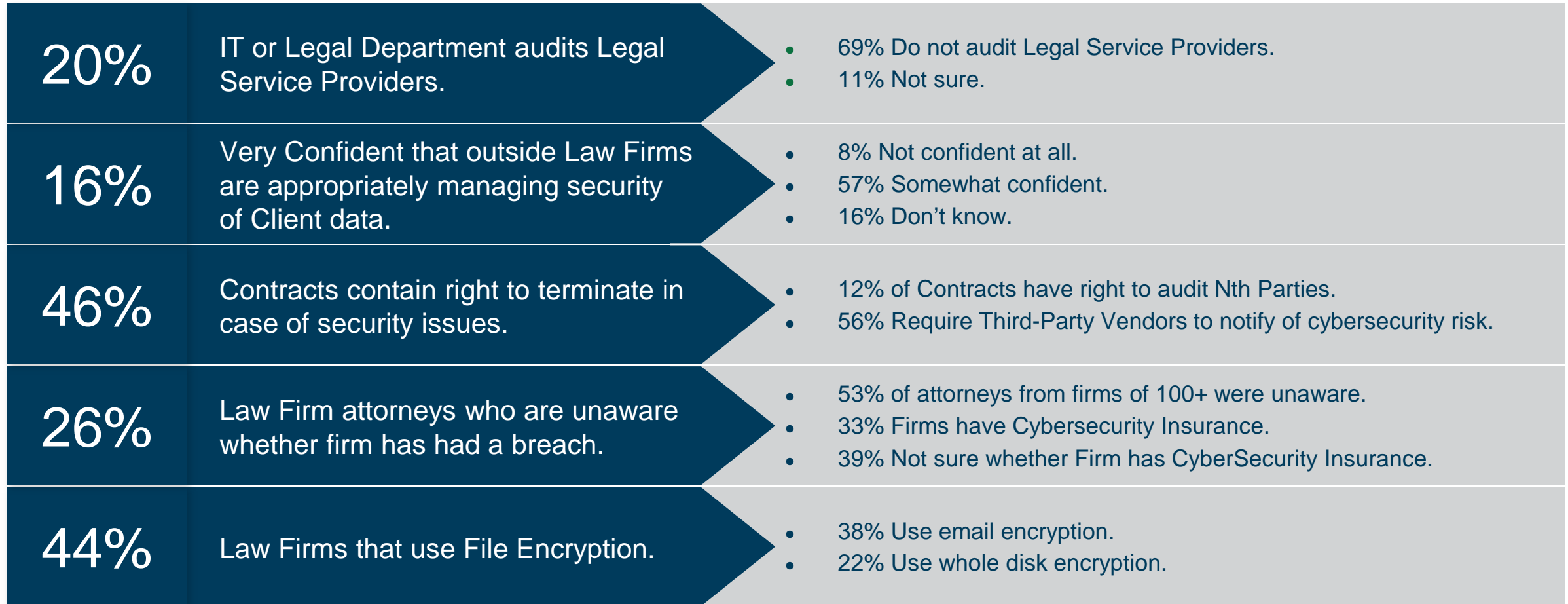


[NIST SP 800-161](#)

# Third Party and Nth Party Risk



# In-House and Outside Counsel Survey Results



[ABA 2019 Cybersecurity Report](#) [ACC Foundation](#)



# Legal Perspective

6%	In-House Counsel report high confidence in Vendors protecting company from cybersecurity risk.	<ul style="list-style-type: none"> <li>• 56% Somewhat confident.</li> <li>• 21% Not at all.</li> <li>• 13% Terminated vendor relationship due to cyber risks.</li> </ul>
12%	Legal departments have In-House Counsel devoted to cybersecurity.	<ul style="list-style-type: none"> <li>• 4% Healthcare / Social Assistance</li> <li>• 7% IT Software and Internet-Related Services</li> <li>• 18% Finance and Banking</li> </ul>
46%	Track mandatory cybersecurity training and attendance for all employees.	<ul style="list-style-type: none"> <li>• 36% Test employees' knowledge of mandatory training.</li> <li>• 33% Do not have mandatory cybersecurity training.</li> <li>• 22% Conduct tabletop exercises.</li> </ul>
23%	Organizations have a Data Map.	<ul style="list-style-type: none"> <li>• 45% Encryption Policy.</li> <li>• 54% Identity and Access Management Policy</li> <li>• 58% Employee Manual Acceptance Policy.</li> </ul>
43%	Conduct a cybersecurity audit of the entire organization at least annually.	<ul style="list-style-type: none"> <li>• 32% Don't know.</li> <li>• 11% Do not conduct a security audit.</li> <li>• 5% Conduct an audit every two (2) years.</li> </ul>

[ACC Foundation](#)



# Increasing Fines and Prescriptive Oversight

<b>FTC</b>	Aggressively protecting consumer information with 20 year oversight.	<ul style="list-style-type: none"><li>• Facebook \$5B.</li><li>• Equifax \$575M</li><li>• LifeLock \$100M</li></ul>
<b>OCR</b>	Increase in total fine compared to Number of Records Breached.	<ul style="list-style-type: none"><li>• Sentara \$2.175M   557 records.</li><li>• TX Health Services Commission \$1.6M   6617 records.</li><li>• University of Rochester Medical Center \$3M   43 records.</li></ul>
<b>GDPR</b>	46 Prosecutions and fines for failure to maintain Article 32 Security Requirements.	<ul style="list-style-type: none"><li>• British Airways £183M.</li><li>• Marriott £100M.</li><li>• €60k Fine for credentials that shared one (1) record.</li></ul>
<b>NY DFS</b>	Detailed data security requirements.	<ul style="list-style-type: none"><li>• Must monitor and oversee Vendors.</li><li>• Assess how Vendors protect Client Information.</li><li>• Conduct Due Diligence for Vendor selection.</li></ul>
<b>CCPA</b>	Reasonable measures   AG points to CIS and NIST Standards.	<ul style="list-style-type: none"><li>• Pending lawsuit against Salesforce regarding eCommerce vendor breach.</li><li>• NIST released new guidance on Supply Chain security.</li></ul>

# Agenda

- Due diligence planning
- Security risk assessments
- Warranties and indemnities
- Operations risk assessments
- Increasing focus
- Security as a service (SaaS) vendor review
- Questions



# Agenda

- **Due diligence planning**
- Security risk assessments
- Warranties and indemnities
- Operations risk assessments
- Increasing focus
- SaaS vendor review
- Questions





## Due Diligence Planning

- Assemble multi-disciplinary team including technical, privacy, security, business, data governance and legal
- Amount and scope will vary on the project
- Prepare a plan and checklist, particularly with larger projects



# Technical Due Diligence: Examples

- Product demos, proof of concept or trial use
- Customer references
- Solution architecture review
- Technical documentation review

# Security Due Diligence: Sample Questions

- How is the data protected via capabilities and policies?
- How is the application or solution protected?
- Does the vendor meet general, industry-specific security and compliance standards?
- Does the vendor meet the unique security requirements of your industry?



# Business Due Diligence: Examples

- Maturity of the SaaS offering
- Contractual requirements: pricing considerations, overage charges and required term or spend commitments
- Review of vendor's legal structure and ownership (public or private, sole or multiple owners, state-of-business formation)
- Financial performance
- Financial status



# Legal Due Diligence: Examples

- Subcontractor relationships
- Reliance on third-party vendors
- Data processing and storage facility locations
- Litigation searches and IP review (any patents that could prevent competitive solutions or customer from taking in house)
- Open source
- Customer audit rights
- Ownership of data
- Outputs such as reports, analytics, etc.



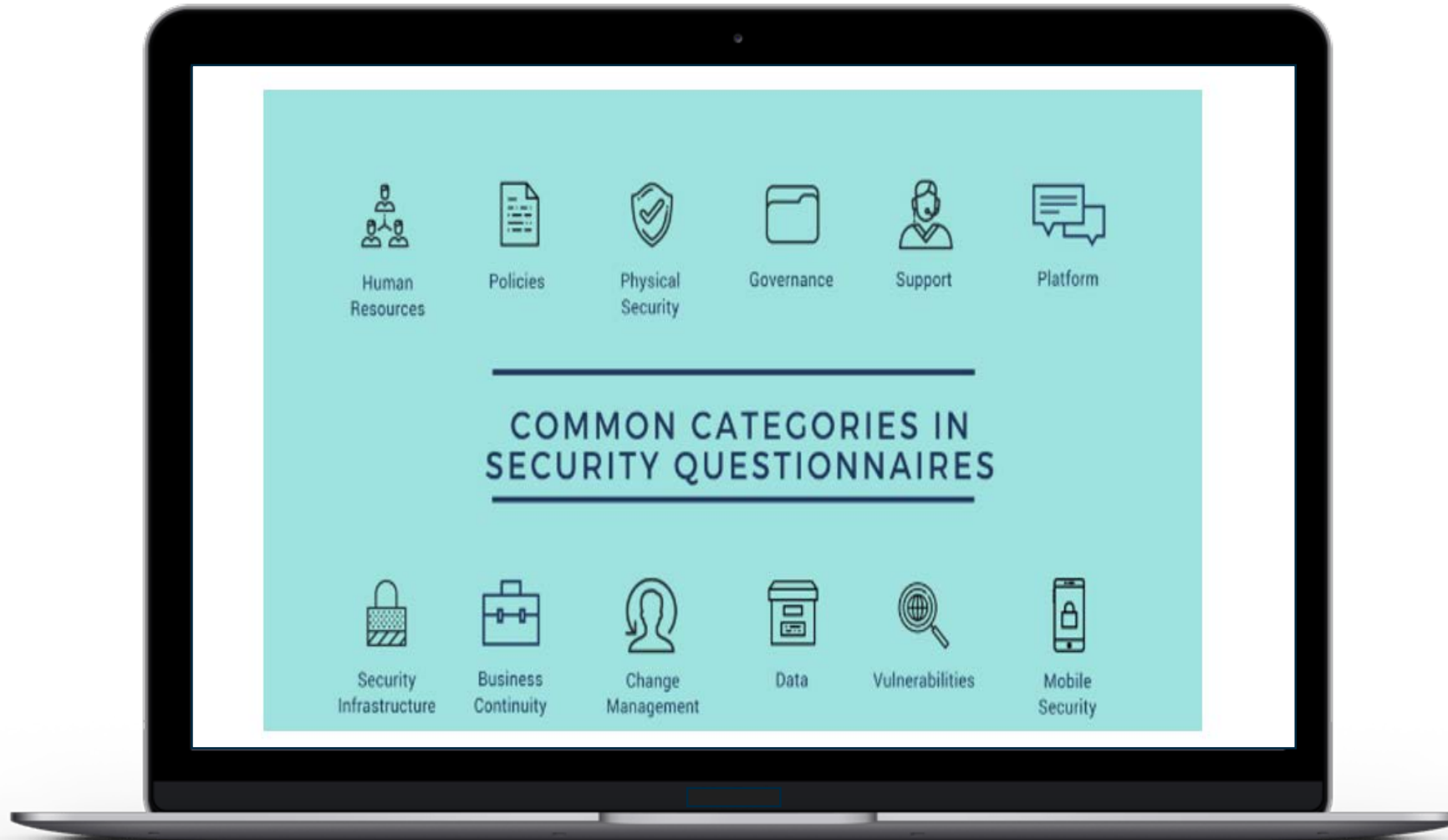
# Potential Risks to Customer's Internal Operations

- Insufficient scoping of implementation
- Business continuity – no plan B
- Access to data assets
- Past data security or privacy breaches by supplier or subcontractors
- Vendor lock-in

# Agenda

- Due diligence planning
- **Security risk assessments**
- Warranties and indemnities
- Operations risk assessments
- Increasing focus
- SaaS vendor review
- Questions

# SaaS Security Risk Assessments



# SaaS Security Risk Assessments

- Does your proposed vendor have independent assessments or certifications such as (SIG, SIG LITE, SOC 2 reports, ISO 27001/27002, HITRUST)?
- In some instances, these certifications and reports may be able to replace security questionnaires.



**HITRUST<sup>®</sup>**

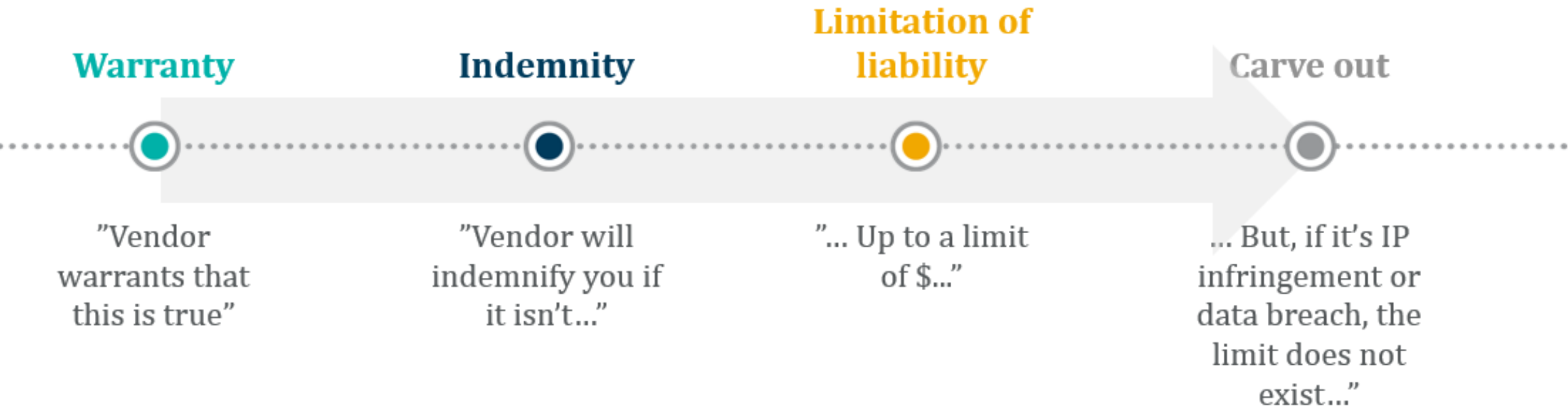




# Agenda

- Due diligence planning
- Security risk assessments
- **Warranties and indemnities**
- Operations risk assessments
- Increasing focus
- SaaS vendor review
- Questions

# Risk Management through Warranty, Indemnity, Limitation of Liability, and Carve-Outs



# Agenda

- Due diligence planning
- Security risk assessments
- Warranties indemnities
- **Operations risk assessments**
- Increasing focus
- SaaS vendor review
- Questions

# Operations Risk Assessments: Vendor Risks

CATEGORY	EXAMPLES	
Information Technology and Security	Privacy breach	Identity fraud
	Intellectual property theft	Data corruption
	Denial or loss of service	Data loss
Financial or Credit	Vendor bankruptcy	Transaction and reporting fraud
	Price or exchange rate instability	Collateral mismanagement
	Unrealized return on investment	Collateral valuation errors
Operations	Business continuity and DR	Safety, OSHA, EPA incident
	Poor quality or performance	Poor customer service or reputation risk
	Damage to assets	Late delivery or theft
Legal	Contract liability	Human resources incident
	Contract dispute	Labor dispute or grievance
	Regulatory action	International law conflict
Brand and Reputation	Brand damage	Communication crisis
	Customer dissatisfaction	Loss of investor confidence
	Competitive pressure	Loss of employee confidence

# Best Practices in Third-Party Governance

**In high performing organizations, Third-Party Governance must be a priority with sufficient resources allocated.**

1. Evaluation of security practices of TP before engaging them.
2. Inventory of all TPs whom you share information.
3. Frequent review of TP management policies and programs.
4. TP notification when data is shared with Nth parties.
5. Oversight by Board of Directors.
6. Formation of TP Risk Management Committee.
7. Visibility into the third and Nth parties with whom you have a direct relationship.
8. Accountability for proper handling of TPRM program.

[\*Ponemon, Data Risk in the Third-Party Ecosystem, 2018\*](#)

# Agenda

- Due diligence planning
- Security risk assessments
- Warranties indemnities
- Operations risk assessments
- **Increasing focus**
- SaaS vendor review
- Questions



# The Future State of Affairs

## Department of Defense – Cybersecurity Maturity Model Certification (CMMC)

- All companies doing business with DoD
- June 2020 target for Requests for Information
- Third-party verification
- All subcontractors
- Allowable, reimbursable cost
- Certificate duration still unknown

## New York State Department of Financial Services

- 23 NYCRR 500
- Financial Institutions and Financial Services Companies
- Very limited exemptions based on revenues and number of employees
- Annual reports by CISO
- Aligns with NIST
- Vendor management policies
- Multi-Factor Authentication

## Sector Specific/Regional Laws

- FTC
- OIG
- GDPR
- CCPA
- NDAA
- PIPEDA
- Brazil and other countries
- “Reasonable Safeguards”

# Cybersecurity Maturity Model Certification

Level	Processes	Hygiene	Description
5	Optimizing	Advanced	Each Practice (171) is documented. A Policy exists that covers all activities. A Plan exists that covers all activities. Activities are reviewed and measured for effectiveness. There is a Standardized, Documented, Approach across all applicable organizational units.
4	Reviewed	Proactive	Each Practice (156) is documented. A Policy exists that covers all activities. A Plan exists that includes all activities. Activities are reviewed and measured for effectiveness. Results of the review are shared with higher level management.
3	Managed	Good	Each Practice (130) is documented. A Policy exists that cover all activities. A Plan exists, is maintained, and resourced that includes all activities.
2	Documented	Intermediate	Each Practice (72) is documented. A policy exists that includes all activities.
1	Performed	Basic	Select Practices (17) are documented where required.

Baseline

Minimum





# NY DFS Requirements

1. Identification and risk assessment of Third-Party Vendors.
2. Minimum cybersecurity practices required by Third-Party Service Providers.
3. Due diligence processes used to evaluate the adequacy of cybersecurity practices of Third-Party Service Providers.
4. Periodic assessment of Third-Party Service Providers based upon risk they present and continued adequacy of their cybersecurity practices.



# Agenda

- Due diligence planning
- Security risk assessments
- Warranties and indemnities
- Operations risk assessments
- Increasing focus
- **SaaS vendor review**
- Questions

# Sample SaaS Vendor Review Questions – The Pop Quiz

- 
- 
- ☐ Do you encrypt in transit and in rest? Are all corporate laptops encrypted?
  - ☐ Are development, production, test environments completely separate from one another?
  - ☐ Is multifactor authentication (MFA) used by the entire company?
  - ☐ Does everyone have single sign on (SSO)?
  - ☐ How difficult are your passwords and how frequently do they need to be changed?
  - ☐ Is a full-time employee in charge of data security?
  - ☐ If you have multiple servers in various locations, how are all the different systems patched? How long does it take to push a patch across the entire enterprise?
  - ☐ Have you had any security incidents or data breaches in the last five years?

# Sample SaaS Vendor Review Questions – The Pop Quiz

- 
- 
- ☐ How do you track and report security incidents?
  - ☐ Is the privacy policy in line with your organization's? Current law?
  - ☐ What are data retention/deletion practices?
  - ☐ How often do you conduct pen and vulnerability testing? What are your policies and practices?
  - ☐ How is customer data segmented, both physically and logically?
  - ☐ What are your backup and disaster recovery policies?
  - ☐ What is your intrusion detection?
  - ☐ What is your SLA/availability/RPO/RTO and what are the remedies for downtime?



# SaaS Vendor Reviews: Best Practices



Follow the data, ask if any other company has access (e.g., contractor, third-party software, data centers).



Review sub-processors and suppliers to understand their role in providing the service and scope of processing your personal data.



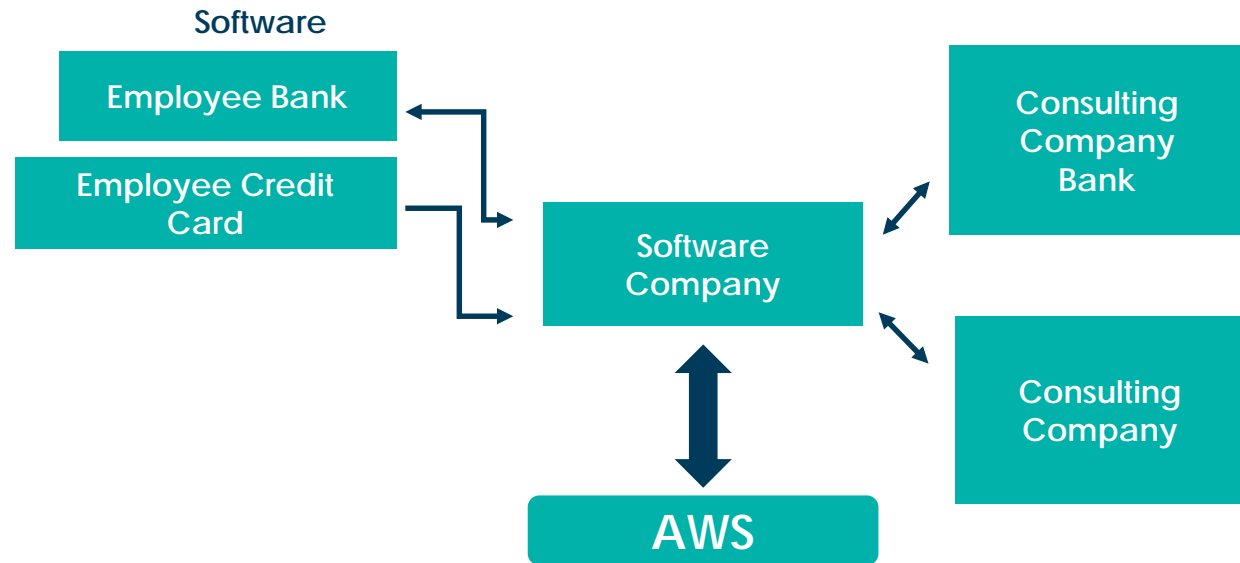
Request certifications at each level. Review them and determine if they have been gerrymandered. Scope can be unreasonably small.



Request meeting with individual who leads security program at each vendor. They may have certifications but not understand them.

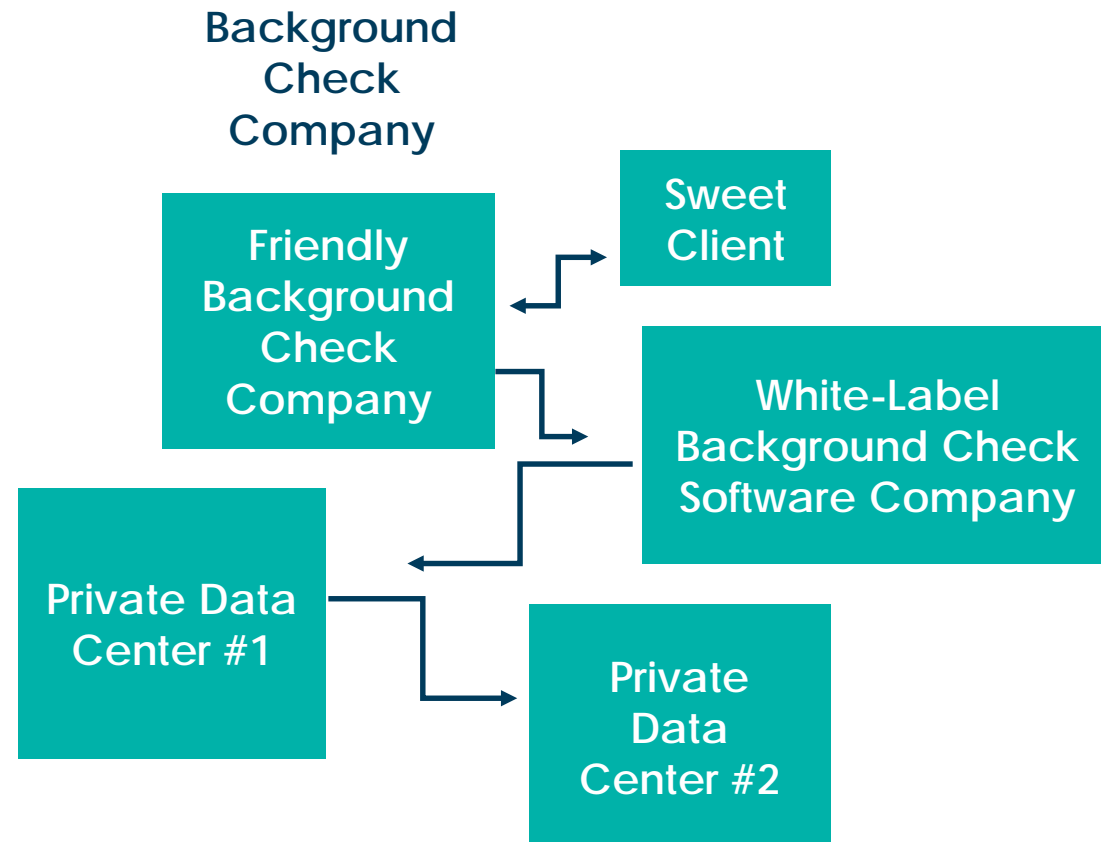
# SaaS Vendor Review Example #1

- Credit card and banking data (PCI).
- Expense Software Company PCI certified.
- PCI report indicated Apple® laptops don't have anti-virus software because Macs do not suffer from viruses.



# SaaS Vendor Review Example #2

- No certifications at Friendly Background Check Company.
- CEO was in charge of IT security.
- White-Label Background Check Software Company not certified.
- DC #1 and DC #2 both SOC 1 certified.
- Software company data on DC #1 and #2 was unencrypted at rest.



## SaaS Vendor Example #3

- Business shortlists 2 vendors
  - Both vendors are small
  - Both sites have no encryption
  - Both vendors rate poorly on BitSight vendor Review
  - Call with security team
- Security and business discuss alternatives

# Agenda

- Due diligence planning
- Security risk assessments
- Warranties and indemnities
- Operations risk assessments
- Increasing focus
- SaaS vendor review
- **Questions**



# Questions?



# Thank You For Attending

**Aparna Dasai Williams**

Senior Director, NortonLifeLock, Inc.

[aparnaMDW@gmail.com](mailto:aparnaMDW@gmail.com)

**Helena M. Ledic**

Associate General Counsel, CSC

[helena.ledic@cscglobal.com](mailto:helena.ledic@cscglobal.com)

**John Bates**

Senior Counsel, Partner Ecosystem,  
CIPP/US, DocuSign

[john.bates@docusign.com](mailto:john.bates@docusign.com)

**Scott Plichta**

Chief Information Security Officer, CSC

[scott.plichta@cscglobal.com](mailto:scott.plichta@cscglobal.com)

