



Session 29: Cybersecurity Risk Update: The Regulatory Bellwether

Moderator:

David Schraub FSA,MAAA,CERA

Presenters:

Nick Lasenko
Alexander Sand



ERM Enterprise
Risk Management
Symposium

Insight Into The Future



Canadian
Institute of
Actuaries



Institut
canadien
des actuaires



SOCIETY OF
ACTUARIES



Enterprise
Risk Management
Symposium

Cybersecurity Risk Update: The Regulatory Bellwether

Session 29
Presenters
Moderator

Friday, April 20 1:45 - 3:00 p.m.
Alexander Sand Nick Lasenko
David Schraub, FSA, CERA, MAAA, AQ

Presenter – Alexander F. L. Sand

Alexander F. L. Sand – Associate, Eversheds Sutherland



Al Sand advises insurers, brokers, banks, payments and digital commerce businesses and other financial services companies on cybersecurity and data privacy matters.

Prior to joining Eversheds Sutherland, Al helped lead cybersecurity initiatives while working at the New York State Department of Financial Services, including the development and drafting of the Department's cybersecurity regulations.

Presenter – Nick Lasenko



Nick Lasenko – Senior Manager, Protiviti (Toronto, Canada)

Nick Lasenko is a Senior Manager in the IT Consulting Security & Privacy practice and has over 10 years of experience managing and leading projects in the areas of IT Security, IT Risk and Audit. Nick's clients have been from a range of industries with a focus on Fortune 500 financial services industry in the US and Canada.

Prior to joining Protiviti Nick was a member of the Assurance practice with KPMG LLP. Nick's experience in public accounting covered an array of industries. Prior to KPMG, Nick had gained industry experience performing various specialized projects as an Analyst with the BMO Financial group.

Presenter and Moderator – David Schraub



David Schraub - Staff Fellow - SOA

David Schraub is the Staff Fellow for Risk Management, Small Company, Marketing and Distribution, Technology and Investment at the Society of Actuaries (SOA) directing volunteer activities in these areas.

Prior to joining the SOA, David worked for life insurance companies and consulting companies in various risk positions, focusing on Solvency II, NAIC ORSA and risk reporting in general. David is a Fellow of the Society of Actuaries, a Chartered Enterprise Risk Analyst of the Society of Actuaries, an Actuaire Qualifie of the Institut des Actuaire (France) and a Member of the American Academy of Actuaries; he graduated from the École Nationale de la Statistique et de l'Administration Économique, one of the French Grandes Ecoles focused on economics, statistics and actuarial sciences.

Contact Information

- Alexander Sand alexanderf.l.sand@eversheds-sutherland.com
- Nick Lasenko nick.lasenko@protiviti.com
- David Schraub dschraub@soa.org

Cybersecurity Risk Update: The Regulatory Bellweather

Friday, April 20, 2018
1:30 p.m. ET



© 2017 Eversheds Sutherland (US) LLP

All Rights Reserved. This communication is for general informational purposes only and is not intended to constitute legal advice or a recommended course of action in any given situation. This communication is not intended to be, and should not be, relied upon by the recipient in making decisions of a legal nature with respect to the issues discussed herein. The recipient is encouraged to consult independent counsel before making any decisions or taking any action concerning the matters in this communication. This communication does not create an attorney-client relationship between Eversheds Sutherland (US) LLP and the recipient. Eversheds Sutherland (US) LLP is part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

Presenter



Alexander F. L. Sand

Associate

alexandersand@eversheds-
sutherland.com

+1 212 287 7019

Our global approach to cybersecurity and privacy

Full spectrum support



- proactive briefing of boards and senior executives
- holistic assessments
- drafting cyber and privacy plans and procedures
- reviewing existing cyber insurance
- table-top exercises



- proactive compliance with multiple jurisdictions (e.g. SEC, NY DFS, GDPR, Chinese law)
- maintenance of relationships
- notifications

- helping manage crisis response
- defense in court and before regulators
- internal investigations
- congressional/parliamentary investigations

- due diligence
- valuation of cybersecurity
- IPOs
- third-party apportionment of cyber risk
- cross-border data transfer agreements

Cyber Threat Landscape and Regulatory Background

Systemic risks and costs:

- As a Lloyd's of London Assessment from last year indicates, cyber risks can extend across sectors, industries and boundaries.

It's not just about data:

- The recent ransomware attacks drive home the point that cyber is not just about exfiltration of data from traditionally data-rich targets, but it's increasingly about theft, disruption and potentially destruction.

Cyber strategy:

- A holistic, proactive, risk-based and well-practiced cyber strategy is required to anticipate risks, mitigate them in advance, and remediate them calmly and expeditiously in the event of a breach.

Regulators share that view:

- At the federal level, the SEC, for example, has indicated its intent to enforce cybersecurity, penalize lack of preparation (and recently spoke of the need to share information).
- Internationally, the GDPR is coming into force this year.
- And in October 2017, the NAIC adopted its Insurance Data Security Model Law, which follows the NYDFS cybersecurity reg. in many ways.

NYDFS Cyber Regulation Bellwether: Compliance Requirements So Far

By now, every Covered Entity should have either:

- Filed a notice of exemption (most are limited exemptions) or
- Decided it must comply with the full regulation

Seven Requirements should be in place:

- A 14-point cybersecurity program
- Written cybersecurity policies and procedures
- A designated CISO
- Limitations on access privileges to information systems with access to nonpublic information
- Qualified cybersecurity personnel with ongoing specialized training
- A written incident response plan
- Notice to the NYDFS Superintendent when a material cyber event occurs

NYDFS Cyber Regulation Bellwether: Recent Compliance Requirements

February 15, 2018:

- Required to certify compliance with current requirements
- Can only certify if fully compliant
- Signed by either the Chairperson of the Board or a Senior Officer

March 1, 2018:

- Penetration Testing and Vulnerability Assessment
- Awareness Training
- Multi-Factor Authentication
- Risk Assessment
- CISO Report to the Board

NYDFS Cyber Regulation Bellwether: Upcoming Compliance Requirements

September 3, 2018:

- Audit Trails
- Application Security
- Limitations on Data Retention
- Monitor Authorized Users and Detect Unauthorized Access
- Encryption

March 1, 2019:

- Third-Party Service Provider Security Policy

Must We Be Our Brothers' Keeper?

If they touch your networks or hold your data, then yes.

Take time to understand all third parties that connect to your networks or have access to your data.

Make sure to apportion risk the right way clearly, and in advance.

Consider other quality control mechanisms – trust, but verify.

NY DFS Cybersecurity Regulation (§500.11) requires written policies be created ensuring that information systems and nonpublic information accessible to third parties is secured.

FFIEC has specifically highlighted the importance of managing external dependencies and document connections with third party service providers, as part of the CAT Tool.

NYDFS Cyber Regulation Bellwether: Vendor Management

- Requires written policies and procedures based on the CE's risk assessment that address:
 - Identifying and assessing the risks of third-party service provider
 - Setting out minimum cyber practices you require
 - Due diligence processes
 - Periodic assessment of the risks of third-party service provider
- Requires a process for vetting third-party service providers and managing their contracts
 - Must be coordinated with the CISO and the cybersecurity program
 - Also coordinated with legal/compliance and with the CISO's Report
 - Escalation procedures

NYDFS Cyber Regulation Bellwether: Vendor Management

- The regulation does not require specific controls to be put in place for all vendors
- But it does emphasize controls that DFS wants you to consider implementing:
 - Establishing **minimum acceptable access control practices**, including the use of multi-factor authentication
 - Mandating the **use of encryption** to protect Nonpublic Information, both in transit and at rest
 - Contractually **requiring vendors to notify you** of cybersecurity incidents impacting your systems or data
 - Including **representations and warranties in vendor contracts** regarding the vendor's cybersecurity practices

Take-Aways for Compliance

Regulators are starting to think differently:

- No longer focused just on consumer data breaches
- Regulators will be increasingly concerned with how financial institutions proactively protect against cybersecurity risks and disruption to critical infrastructure
- More regulation and enforcement is coming, and cross-jurisdictional issues will be significant

What to do about it:

- Be proactive on evolving cybersecurity issues
- Take a risk-based approach
- Be substantive, not just focused on base-line compliance
- Develop a clear picture of how your cybersecurity operations are structured
- Leverage existing ERM functions
- Make sure it all works together



Alexander F. L. Sand

Associate

alexandersand@eversheds-sutherland.com

+1 212 287 7019



CYBERSECURITY RISK UPDATE: THE REGULATORY BELLWETHER CYBERSECURITY & PRIVACY

FRIDAY, APRIL 20, 2018
1:30 P.M. ET

PRESENTER: NICK LASENKO


PROTIVITI AT A GLANCE

Protiviti Overview

Protiviti is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Cybersecurity clients include:

 **Two Thirds** of Top 30 U.S. Banks

 **Over 50 %** of 13 Fortune 100 Insurance Firms

Geographic coverage

North America, Europe, Central America, South America, Asia and Australia

Financial Services

is Protiviti's largest industry segment

70+

offices worldwide in 20 countries

4,000+
professionals

Global FSI Cybersecurity Practice

Our global Financial Services practice enables seamless delivery across geographies.

- Over 350 security practitioners with real-world FSI experience
- One company; not limited by partnership legal structures
- Uniform go-to-market and client service model
- Provide robust solutions with clear business drivers
- Leading edge technical capabilities
- Ability to provide clients with the best talent and service levels

Market Recognition



A Top 5 Firm in the Kennedy Vanguard of Financial Services Risk Consulting Providers



8 Protiviti consultants were named in *Consulting magazine's* list of Top 25 Consultants in the last 8 years



GARTNER'S MAGIC QUADRANT **Challenger** —positioned by Gartner, Inc. in the December 2016 Magic Quadrant for Operational Risk Management Solutions.



2015 - 2017 Fortune 100 Best Companies to Work For®

SECURITY AND PRIVACY SOLUTIONS

Protiviti's knowledgeable professionals have decades of experience working with Financial Services clients across our Security and Privacy solutions. Our team is able to address even the most challenging business issues. **We have deep competency in the following areas:**

Data Security & Privacy Services

- **Trending Regulatory topics (NYDFS Cybersecurity, GDPR, etc.).**
- Payment Card Industry (PCI) Activities
- Vendor Security Risk Management

Security Program & Policy Services

- Cyber Program Office Offering
- Cyber Program Intelligence (Board Reporting and Key Risk Indicators)
- Security Benchmarking and Roadmap Activities

Vulnerability / Pen Testing Services

- Red Teaming
- IOT Security (including Medical Devices)
- Technical Security Assessments across the Entire Technology Stack (Infrastructure, Database Application, Web Application, Mobile, etc.)

Incident Response and Forensic Services

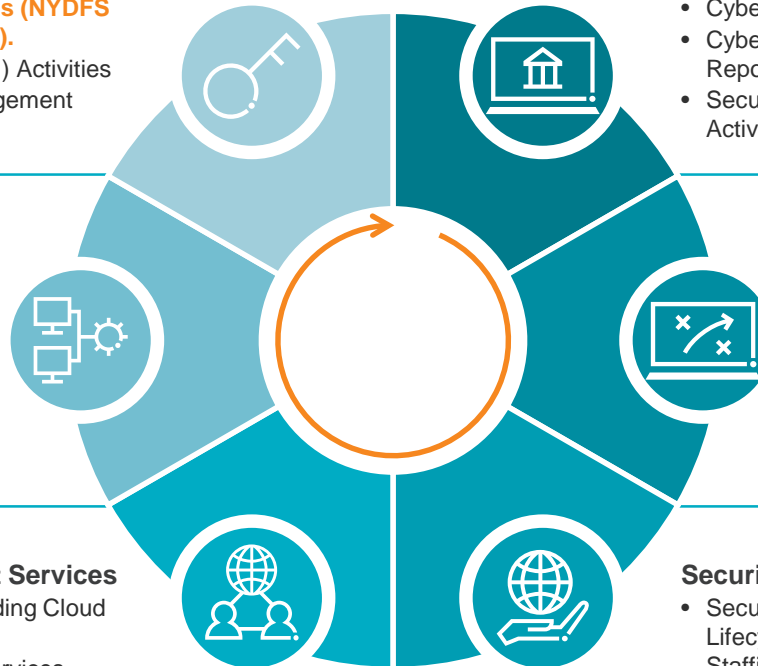
- Breach Response and Forensic Services
- Cyber War Gaming and Table Top Exercises

Identity and Access Management Services

- Identity Management Strategy (including Cloud and Customer Facing Efforts)
- IDAM Design and Implementation Services (including SalePoint and Other Emerging Technologies)
- Privileged Access Management Solutions (CyberArk)

Security Operations Services

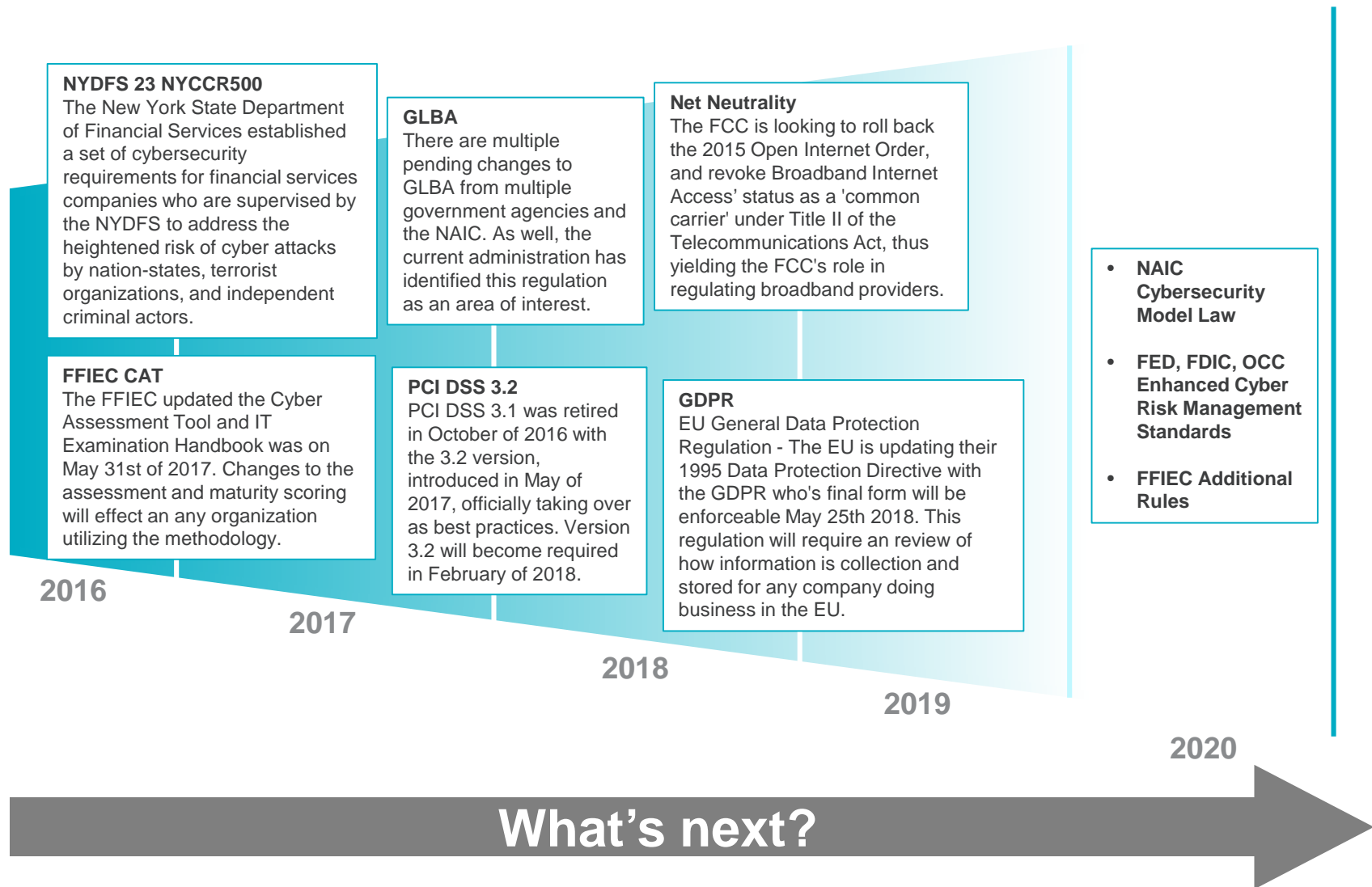
- Security Operations Support across the Lifecycle (Strategy, Design, Implementation, Staffing)
- Enterprise Operations Center and Other Integrated Solutions





REGULATORY ENVIRONMENT

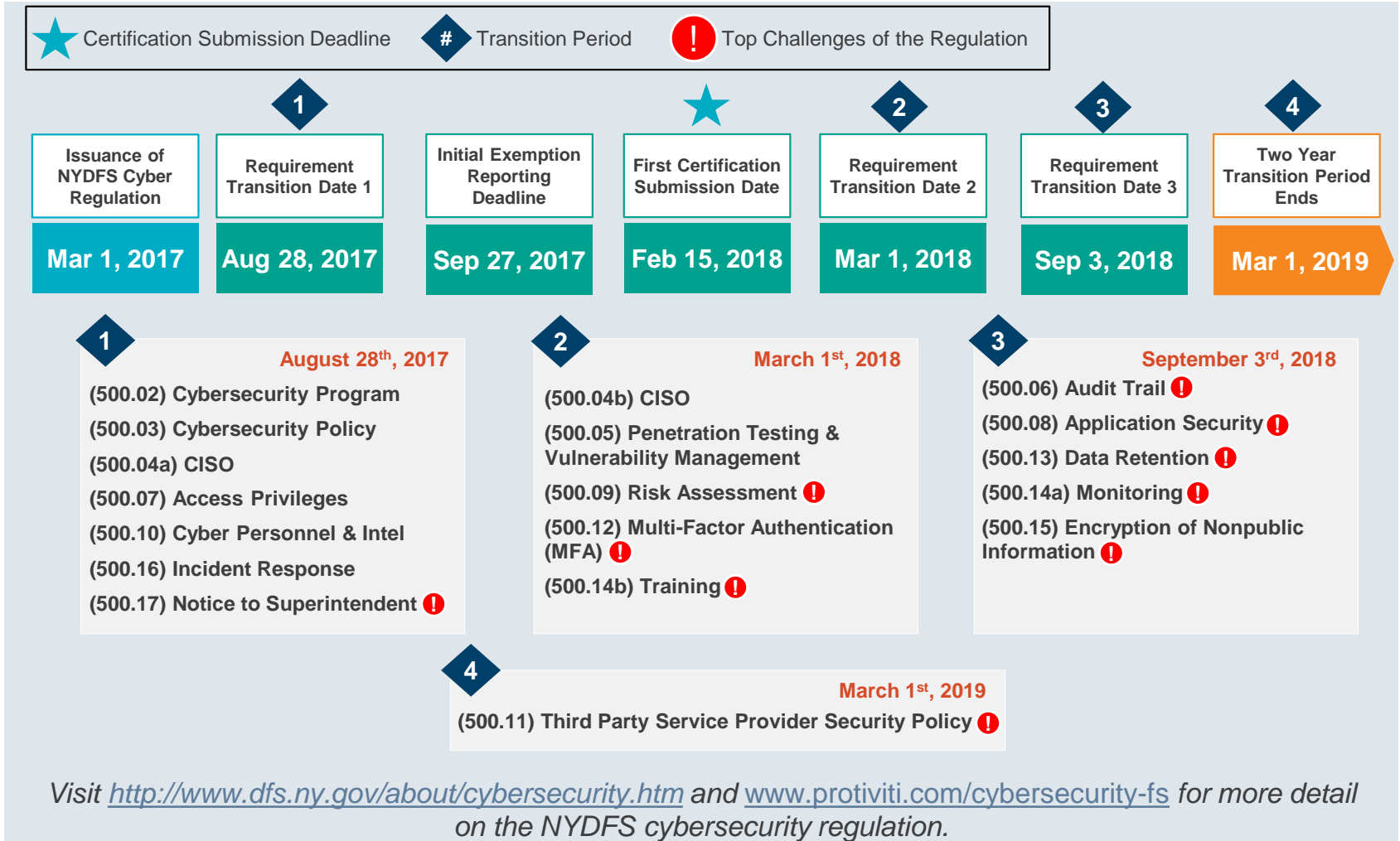
GLOBAL REGULATORY ENVIRONMENT CHANGES





NYDFS

NYDFS CYBERSECURITY REGULATION KEY DATES



EXAMPLES OF IMPLEMENTATION CHALLENGES (1/3)



Disparate Standards

- Particularly for FBOs*, but true for any institution that operates across state and national boundaries, need to **reconcile different regulatory standards**



Risk Assessment

- Expertise to execute and balance between **aligning the program to risk**, while appeasing regulators



Certification

- Determining the **right parties** to certify and sub-certify



Encryption of Nonpublic Personal Information

- Important control, but can slow down processing or cause recovery issues – this will need to be **planned**

*Foreign Banking Organizations

EXAMPLES OF IMPLEMENTATION CHALLENGES (2/3)



Multi Factor Authentication

- Organizations are in early stages of implementing multi-factor authentication
- Implementation includes **cultural** and technical changes



Application Security

- Protiviti's recent S&P survey indicates only **29% of companies** have technical controls to enforce application security in the development process



Data Retention and Destruction

- Aligning **current** practices with requirements



Third Party Risk Challenges

- Assessing and performing due diligence on a **large population of third parties**

EXAMPLES OF IMPLEMENTATION CHALLENGES (3/3)



Monitoring Requirements

- Monitoring requirements are increasing
- Closing the time to detect that a breach occurred – recent surveys indicate **100+ days between initial breach and activity detection**



Audit Trail

- Determining what **role Internal Audit plays** in testing compliance



Body of Evidence

- Compiling the appropriate **documentation** to support certification



Program Sustainability

- Account for **your control maturity** and sustainability; controls may breakdown over time

GDPR READINESS ASSESSMENT



Client Need

Insurance company with operations in the European Union, was in need of experienced information security knowledge to provide strategic guidance and support to address the GDPR. The client required development of a data inventory and framework to identify information systems and third parties in scope for the GDPR.



Protiviti Approach

1. Interviewed key departmental stakeholders, reviewed current policies/procedures and evaluated vendor contracts to identify Client GDPR obligations, current state and gaps
2. Developed a GDPR Current State Summary Report
3. Developed a GDPR Gap Analysis Report that identified key gaps, pain points and root causes
4. Developed Vendor contract review assessment template and GDPR DPIA template framework and approach

Benefits Achieved

Delivered a cohesive GDPR Roadmap including prioritized projects based on GDPR obligations, key focus areas and governance program enhancements

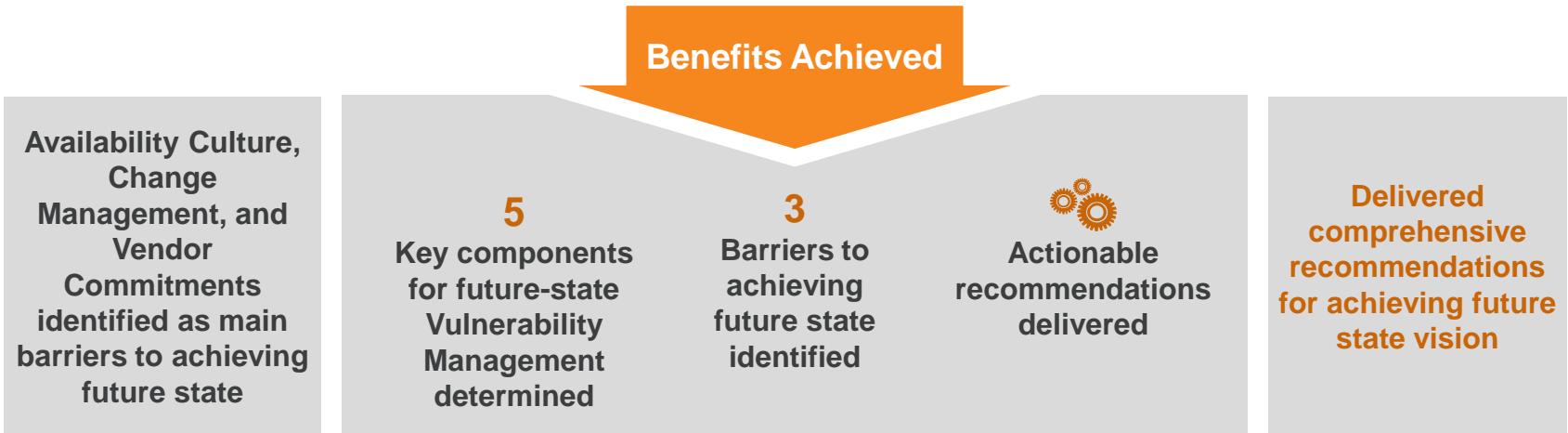
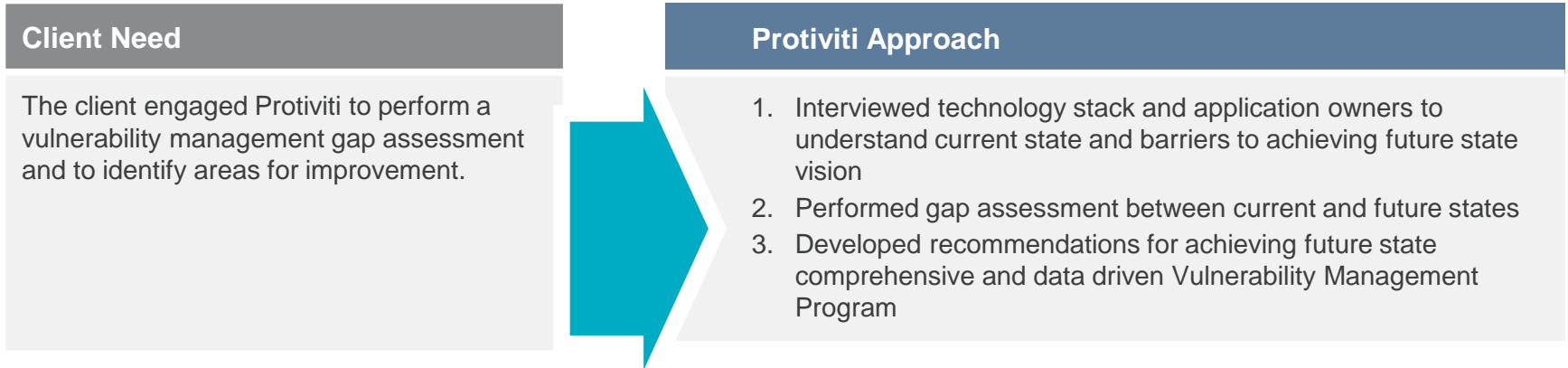
Increased enterprise awareness of the GDPR

64
Information systems and third parties identified as in-scope for the GDPR

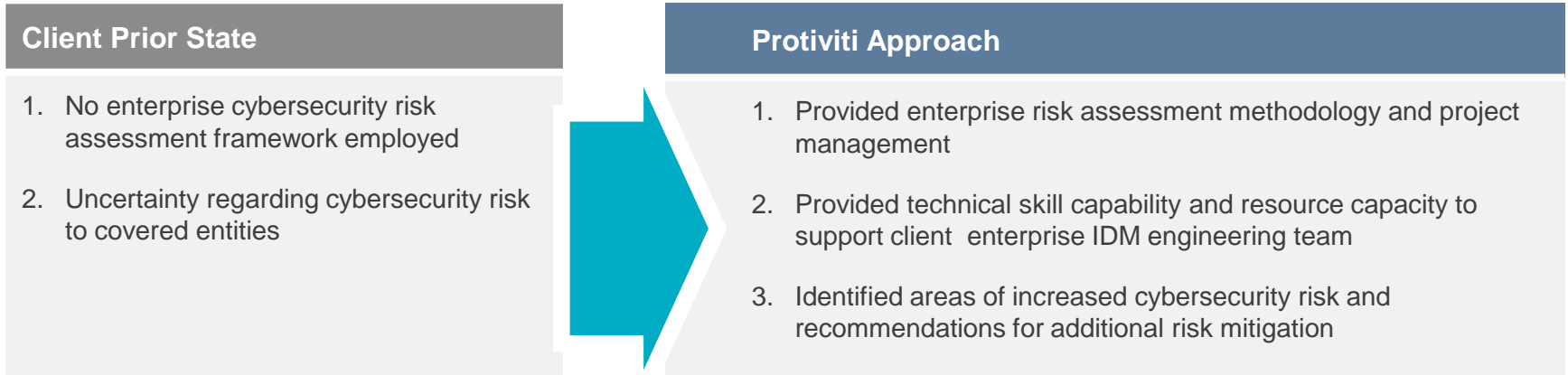
Developed GDPR best practices to improve current data management standard and privacy policy

Development of data inventory justified creation of a formal data governance program

VULNERABILITY MANAGEMENT OPTIMIZATION



NYDFS RISK ASSESSMENT



Benefits Achieved





BONUS: GDPR

OVERVIEW



What is GDPR?

- General Data Protection Regulation
- Replaces local EU Data Protection Directive implementations (e.g., in UK the “Data Protection Act”)
- **Starts on May 25, 2018**



Who is Subject?

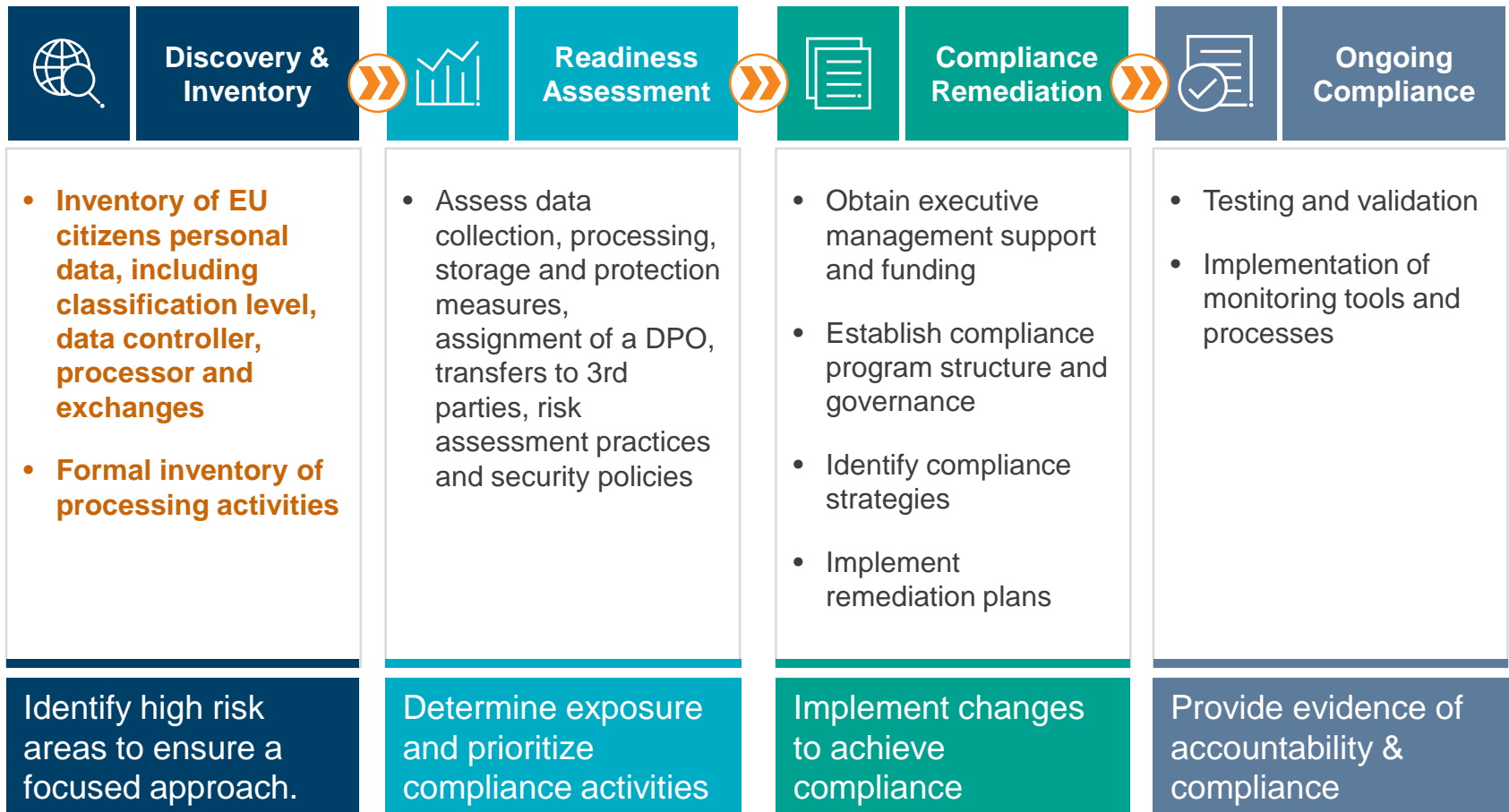
- **All organizations that collect and process personal data of EU data subjects** – regardless of size
- No longer applies only to organizations with an office the EU - **is borderless**
- **Applies to data processors** - not just data controllers



What are the Penalties?

- Up to 20M € or 4% of organization’s annual global turnover, whichever is higher (board attention is now guaranteed)
- Data subjects can claim **compensation for damages** from breaches to their personal data

APPROACH TO GDPR COMPLIANCE



Phase duration and level of effort is highly dependent on personal data processed, the size and scope of your environment and process complexity and maturity.

Face the Future with Confidence

Questions



Contact Information

- Alexander Sand alexanderf.l.sand@eversheds-sutherland.com
- Nick Lasenko nick.lasenko@protiviti.com
- David Schraub dschraub@soa.org