imperva

Driving Digital Transformation While Mitigating Risks And Ensuring Compliance

Terry Ray
SVP and Imperva Fellow

Agenda

- Challenges with Digital Transformation
- Traditional Security Approach
- Risk Assessment Approach
- How Imperva can Help
- Q&A

Challenges with Digital Transformation

Transformation is Happening

Drive revenue vs. Reduce cost

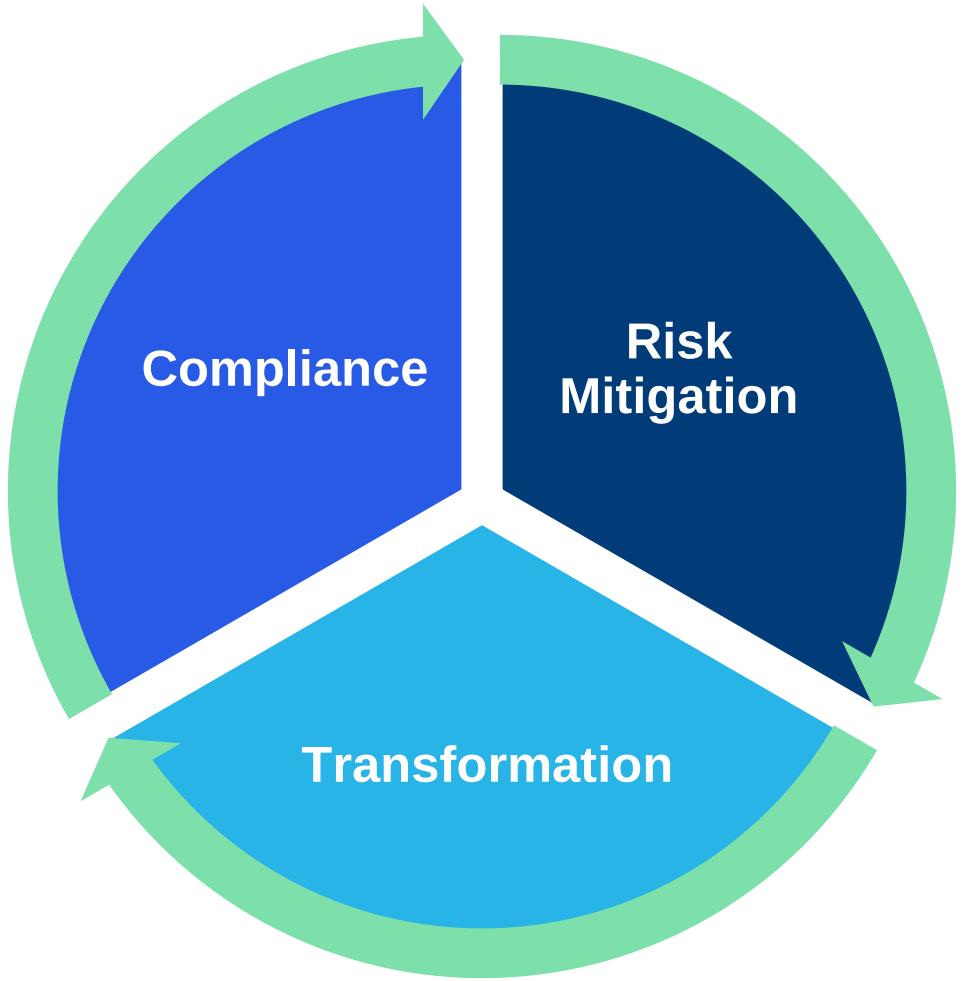
Risks

- Unnoticed attacks
- Too much data, EVERYWHERE
- Lack of visibility into who accesses what data, how
- No assurance in existing controls
- Security isn’t part of DevOps

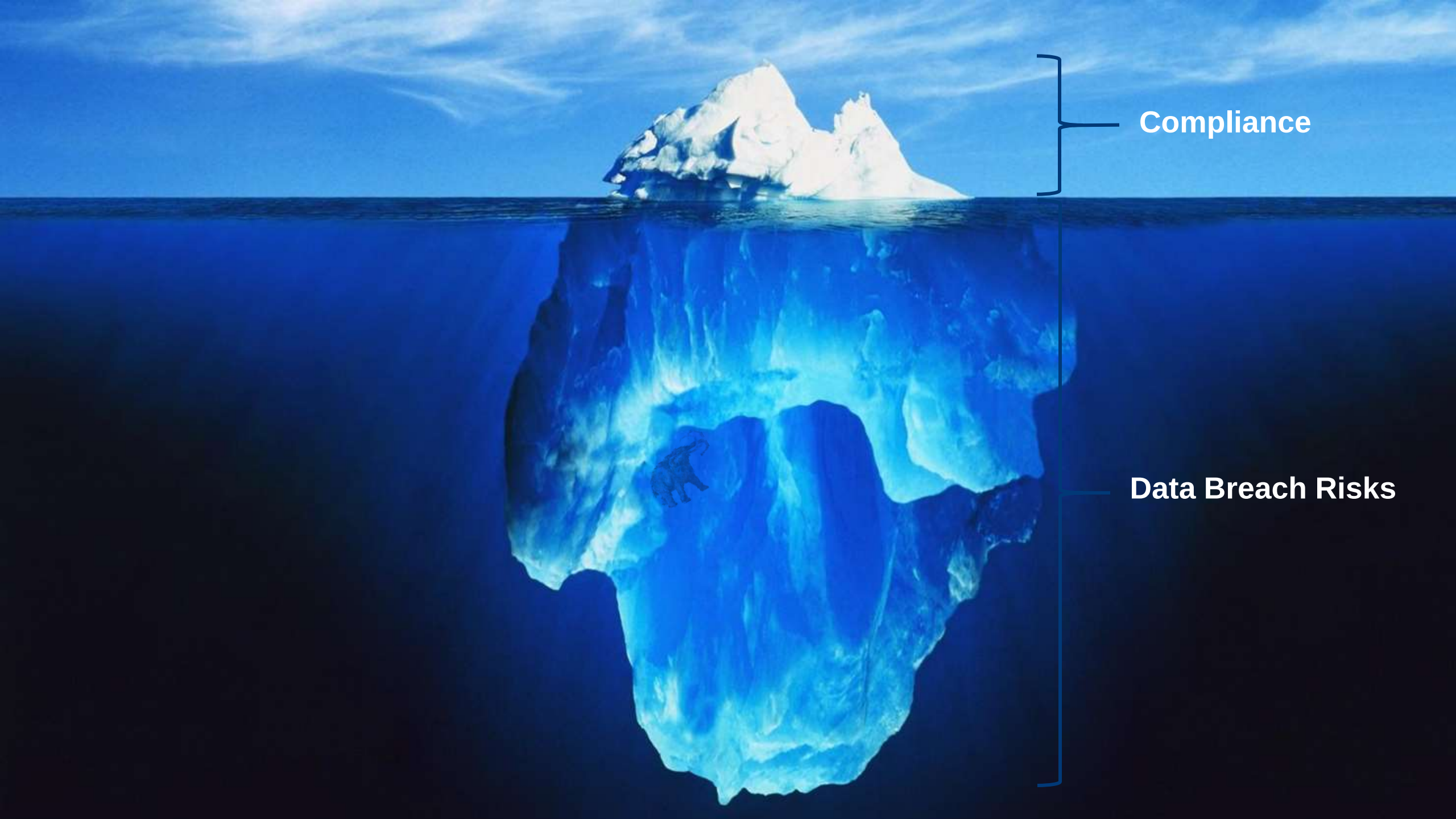
Pressures in Financial Services Industry

Risk Mitigation, Transformation, Compliance

- Innovative Fintech models
- Big Tech
- Open Banking



- Complex legacy system
- Digital application
- Cloud adoption
- More data, EVERYWHERE
- Increased competition
- Stricter regulations


Compliance
Data Breach Risks

Why is Detection so Difficult

More legitimate data access

34% of workers said they share passwords or accounts with their coworkers[1]

Incident overload and alert fatigue

54% of companies admitted that they tend to ignore security alerts[2]

Lack of skilled security professional

70% of CISOs consider it their top concern[3]

Insider threats

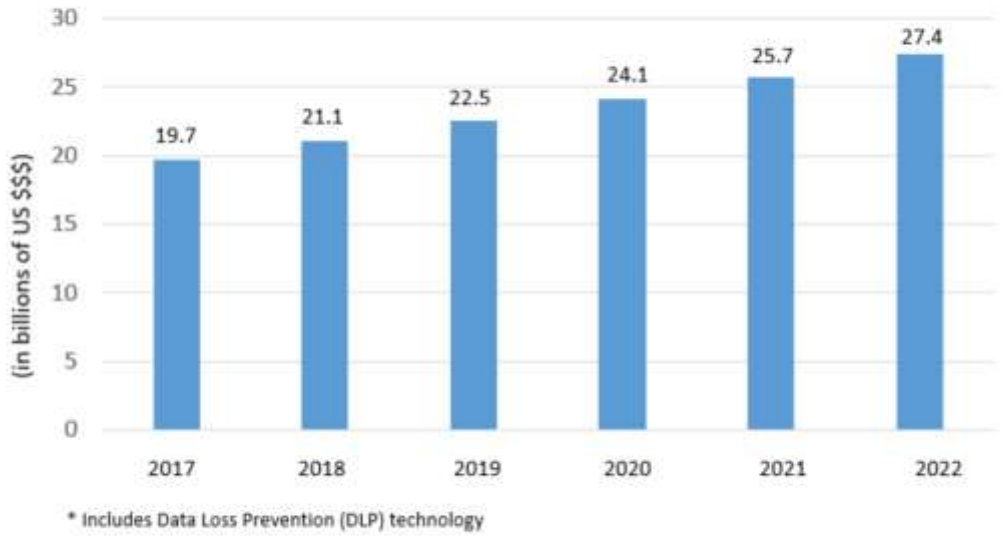
Fraud is the most frequent insider threat incident type for financial services[4]

Source:
[1] https://www.techradar.com/uk/news/the-dangers-of-password-sharing-at-work
[2] Security Operations Challenges, Priorities, and Strategies, ESG, 2017
[3] What CISOs worry about in 2018, Ponemon Institute, 2018
[4] CERT National Insider Threat Center, 2019

Traditional Security Approach

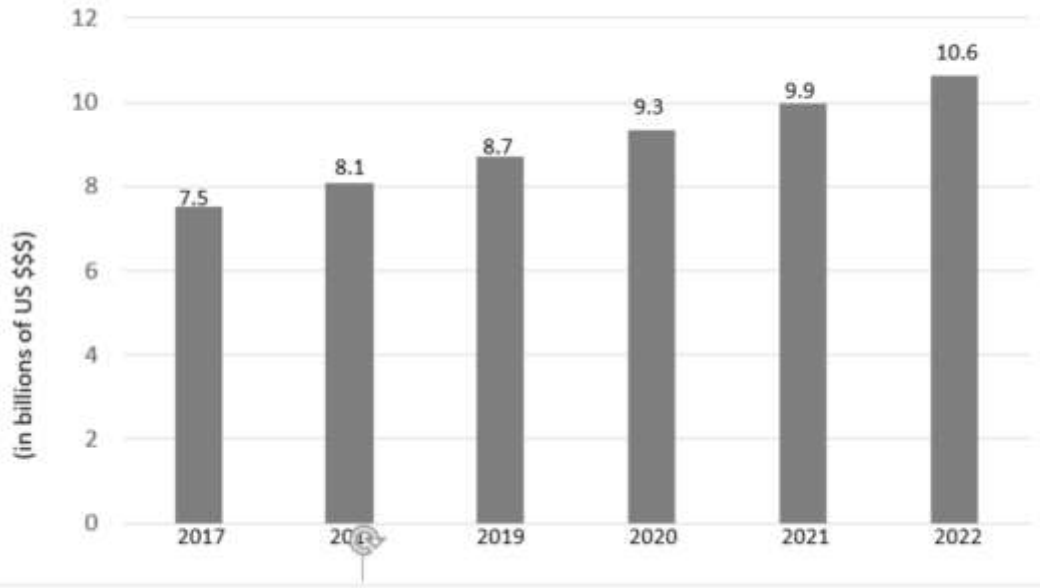
Security Spending

Figure 1: Edge security market forecast*



Source: Ovum *Software Market Forecasts: Security, 2017–22*

Figure 2: Core security market forecast



Source: Ovum *Software Market Forecasts: Security, 2017–22*

Spending in Perimeter-based & Identity-based security continues to grow

Challenges of Traditional Security Approach

Perimeter-based Security

- Ex: Endpoint, network security
- False assumption: “Trusted” internal network where data is safe
- Can’t protect against insider threats
- Fail to empower a digital workforce to better serve customers while protecting data

Identity & Access Management

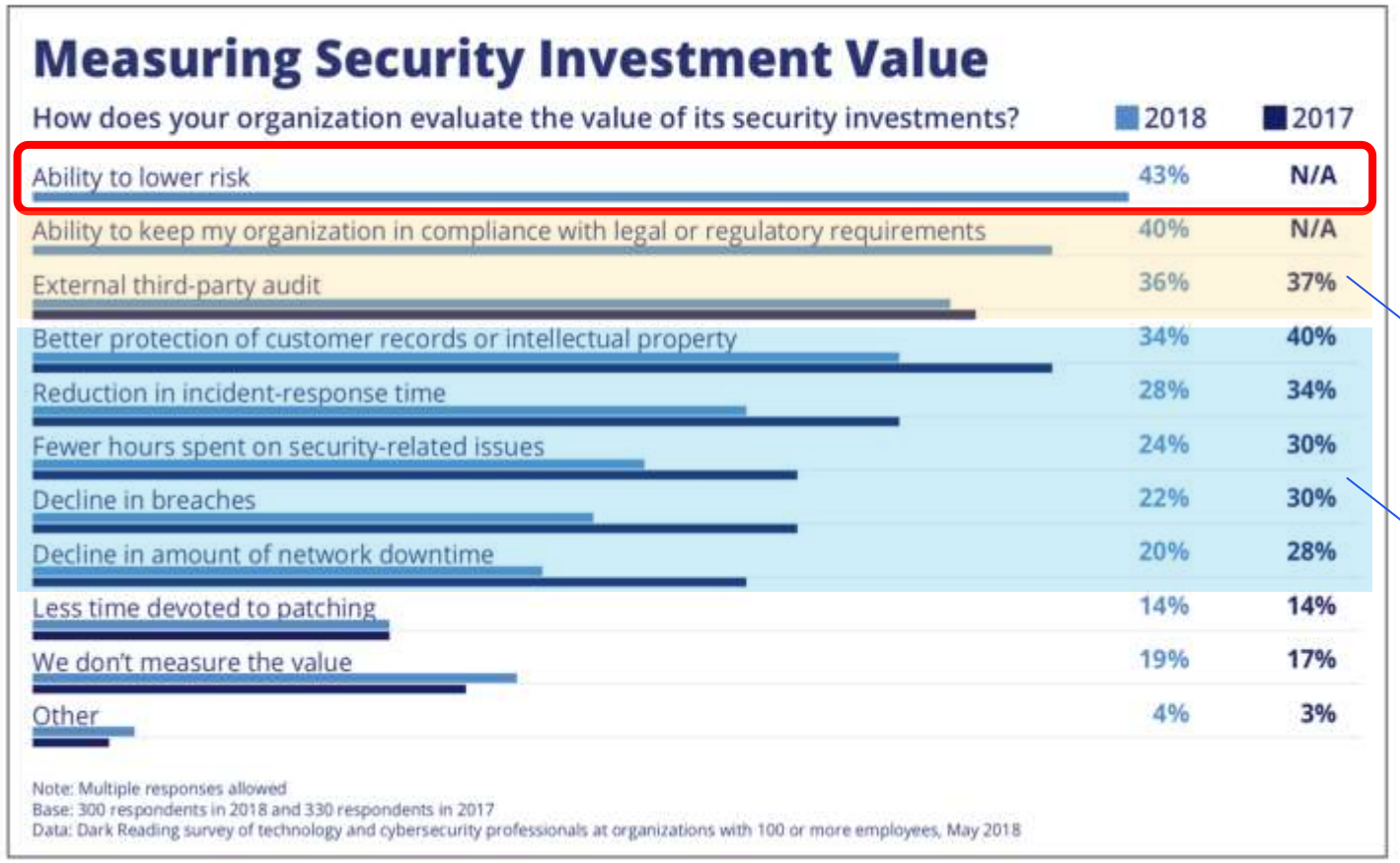
- Ex: User authentication
- Identity-aware is a must but not sufficient
- Not designed to detect breaches but to make decisions whether to enable access
- Can’t protect against insider threats

Data Breaches Still Happen

Risk Assessment Approach

Taking a Risk Assessment Approach

Figure 1



- Most organizations are evaluating the value of their security investments based on **Ability to lower risk**

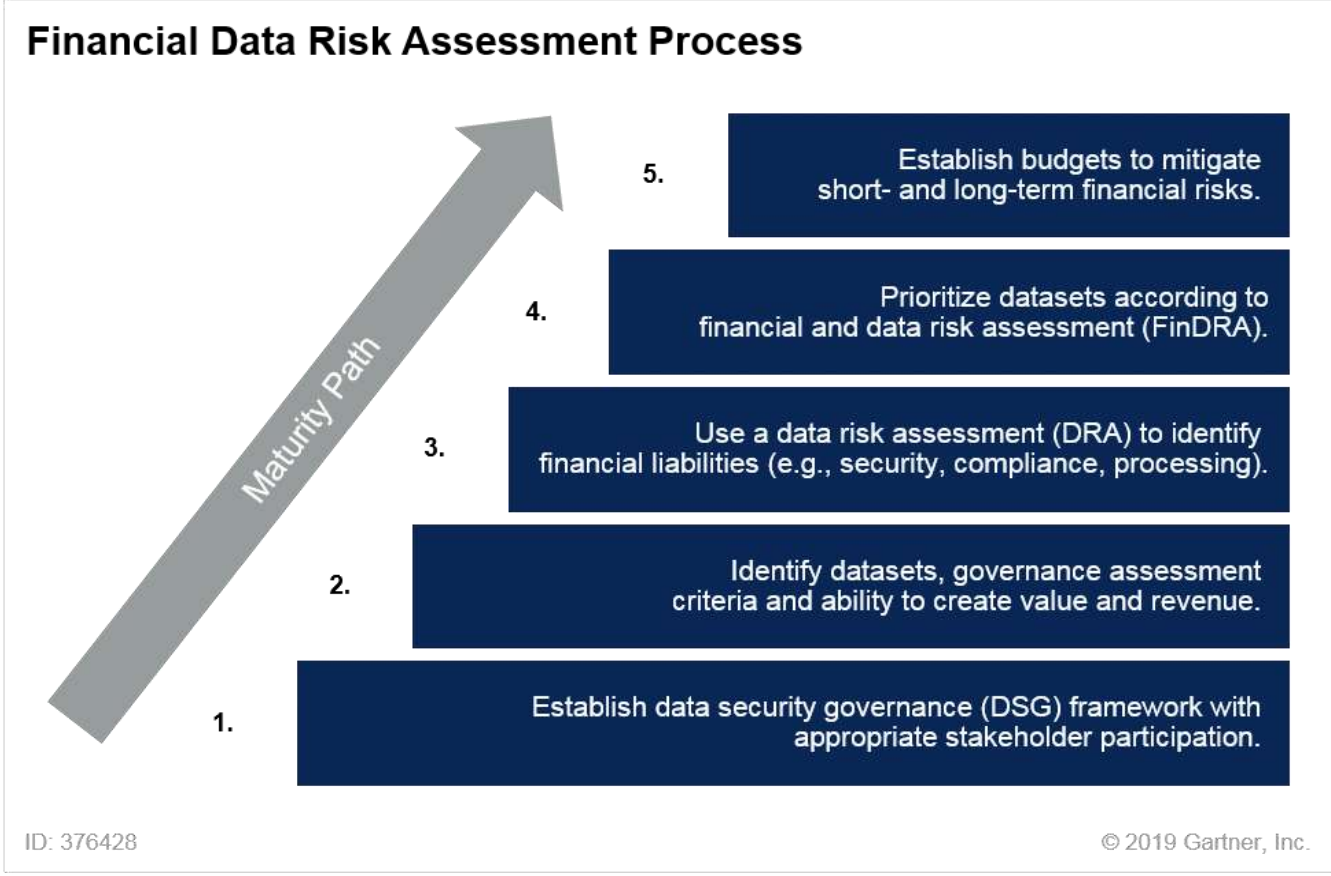
Compliance related

Security related

Source: Dark Reading Report, 2018

imperva

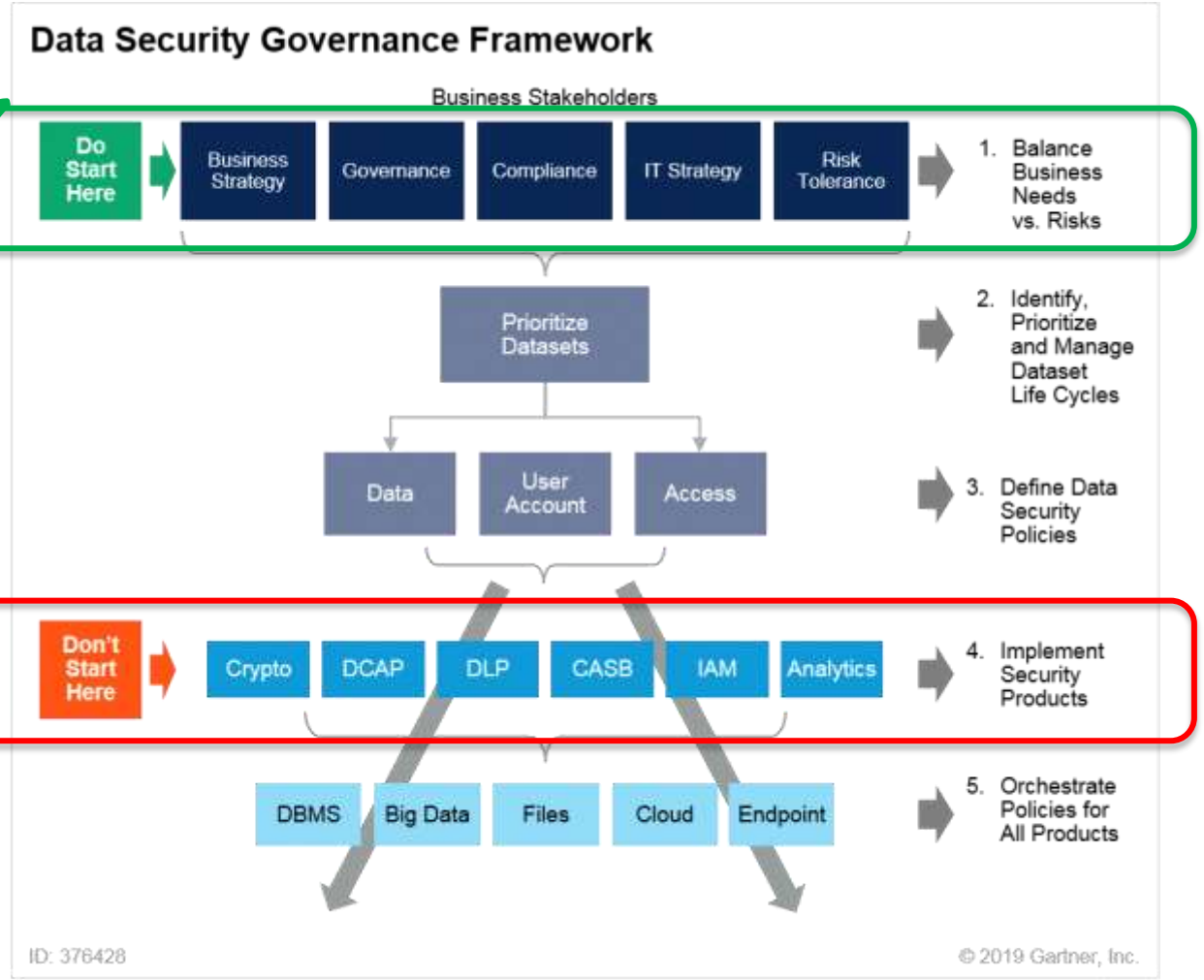
Example: Gartner Risk Assessment Framework



- **Get alignment** with key stakeholders
- **Priority** = Identify assets + Assess liabilities
- **Security** = Mitigate prioritized risks

Source: Develop a Financial Risk Assessment for Data Using Infonomics, Gartner 2018

Example: Gartner Risk Assessment Framework



- Start with balancing between **business needs** and **risks**
- Don’t jump to security products/solutions
- Enforce **consistent policies** across hybrid environment

Source: Develop a Financial Risk Assessment for Data Using Infonomics, Gartner 2018

imperva

To Keep or not to Keep

Source: Gartner (January 2019)

- Maintaining and securing data here is a no-brainer

- **The Problem is:**
  - Is there any data that you truly don't care?
  - If so, can you delete it?

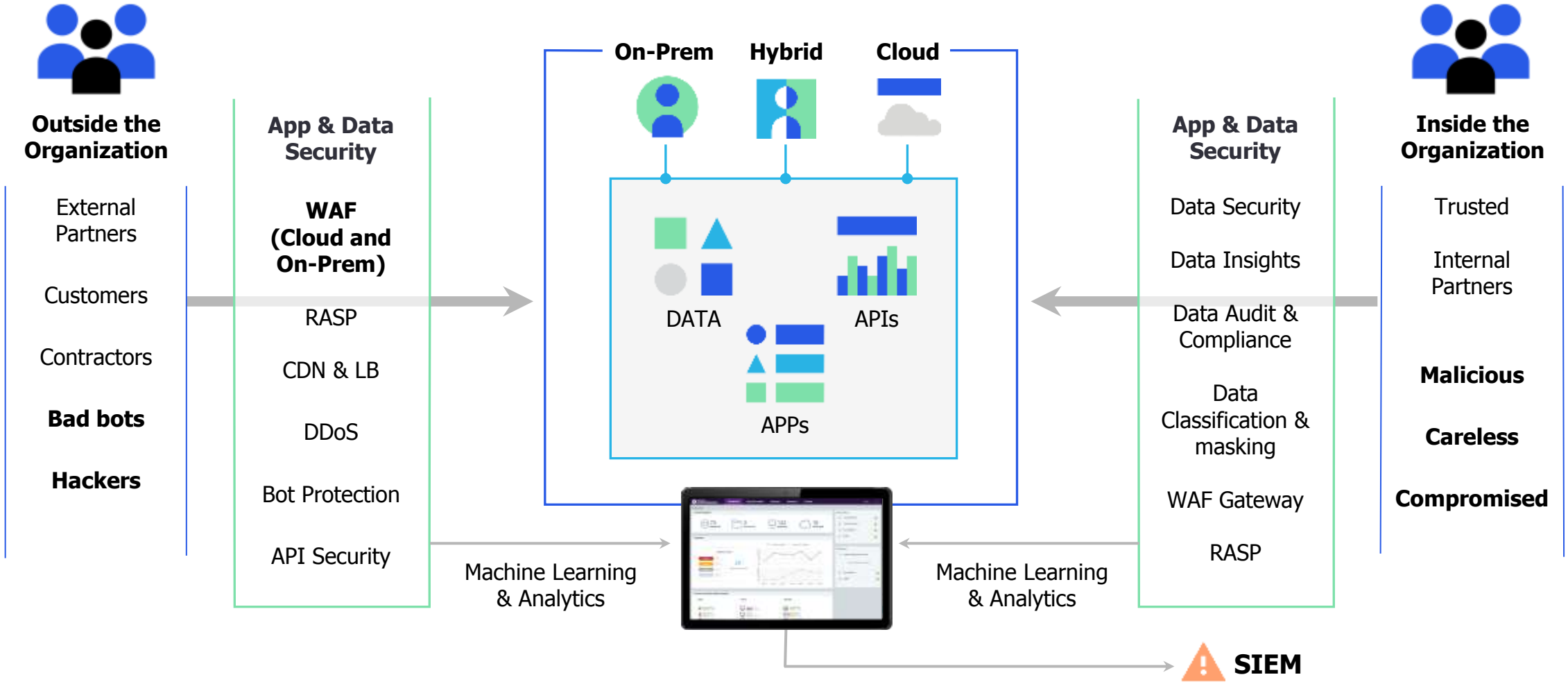
Source: Develop a Financial Risk Assessment for Data Using Infonomics, Gartner 2018

Enabling Digital Transformation while Mitigating Risks

Data Security is a Must

> **“As the business becomes digital, security must become Data-Centric”**
>
> – **Forrester Research, 2018**

Imperva Security Defense In Depth Architecture



**Internal API Security is planned for 2020*

imperva

Example: Buy Down Risks with Data Security

Financial Services

Exposure of 100 million unique customer records (e.g. PII)

If a breach happens…

All users in the system have to be notified

A physical mail costs $0.5 = $50 M

Fines (e.g. GDPR non-compliant)

Lawsuit

Loss of clients/vital data/productivity

Damage to reputation

Damage to business relationships

= **>$50M**

- Data access control
  - Single query should not exceed 10,000 PII records

→ Limits application compromise down to 10,000 PII records = $20,000

- Identify suspicious data access
  - Service account abuse
  - Massive data records access
  - Sensitive data access

→ Improve breach prevention

- Masking sensitive data
  - Reduce attack surface in non-production environment

→ Prevent data breach risks in non-prod. environments

Result: Buying down **~$50M**

imperva

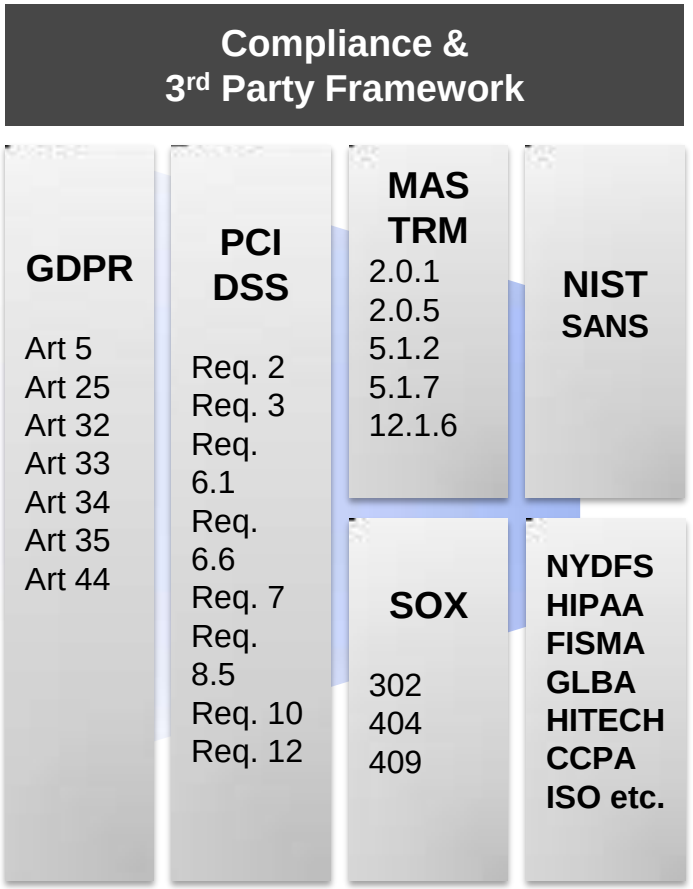
Key Takeaways- Start with What Matters Most

DATA

- Do you know **where** your sensitive data is?
- Can you tell **who accesses what data**, and **how that data is used**?
- Can you determine which **data access is appropriate**?
- Can you **detect suspicious data access** with high confidence?
- Do you have the **necessary records** for **incident response**?

APPS

- Do you detect and and mitigate **application vulnerabilities**?
- Are **vulnerable apps taken offline** or is the risk accepted?
- Can your organization tolerate a **DDoS longer than hours**?
- Does your **app security strategy up level periodically** to detect changing attack methods (i.e. Crypto-Jacking, ransomware)?



Q&A

Thank You

Terry Ray