peters & associates
simplify solve succeed

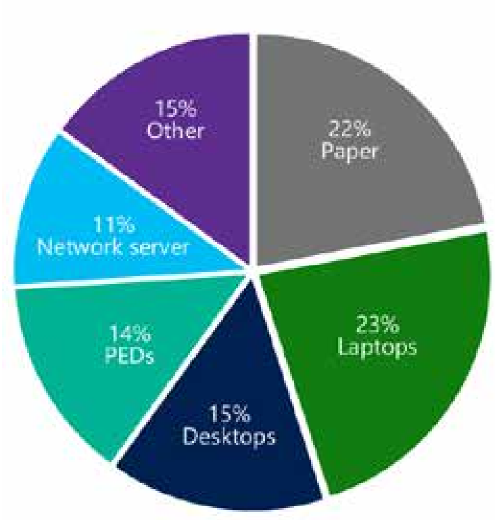
Staying Ahead of Cybercriminals - Why You Need a Data Centric Risk-Based Approach

Timothy O’Hara, CPA, CGMA

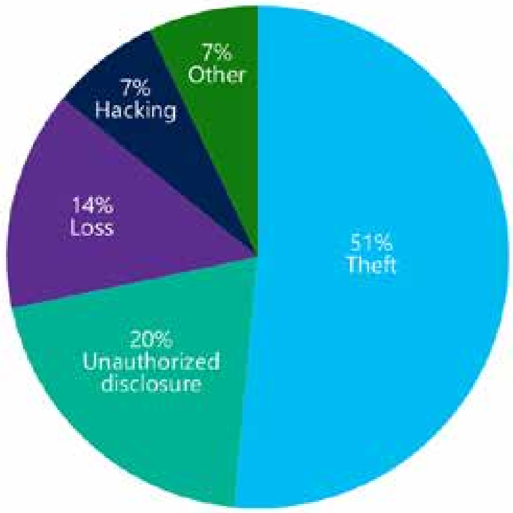
August 4, 2017

If you keep up on current events, you already know cyber threats are increasing, not only in frequency, but also in severity. Threat actors have adjusted their strategies to circumnavigate traditional security defense models and methods. Meanwhile, the age-old concept of building protective systems around data at rest is simply ineffective in the today’s workplace. Data protection models need to support work from anywhere e.g. Cloud, Bring Your Own Device (BYOD), Mobility, and The Internet of Things (IoT).

A multi-year breach summary report of the healthcare industry, by the Health and Human Services Department, shows change in the industry as data spans multiple device types and multiple threat vectors:



Breach Types By Device



Breach Types By Act

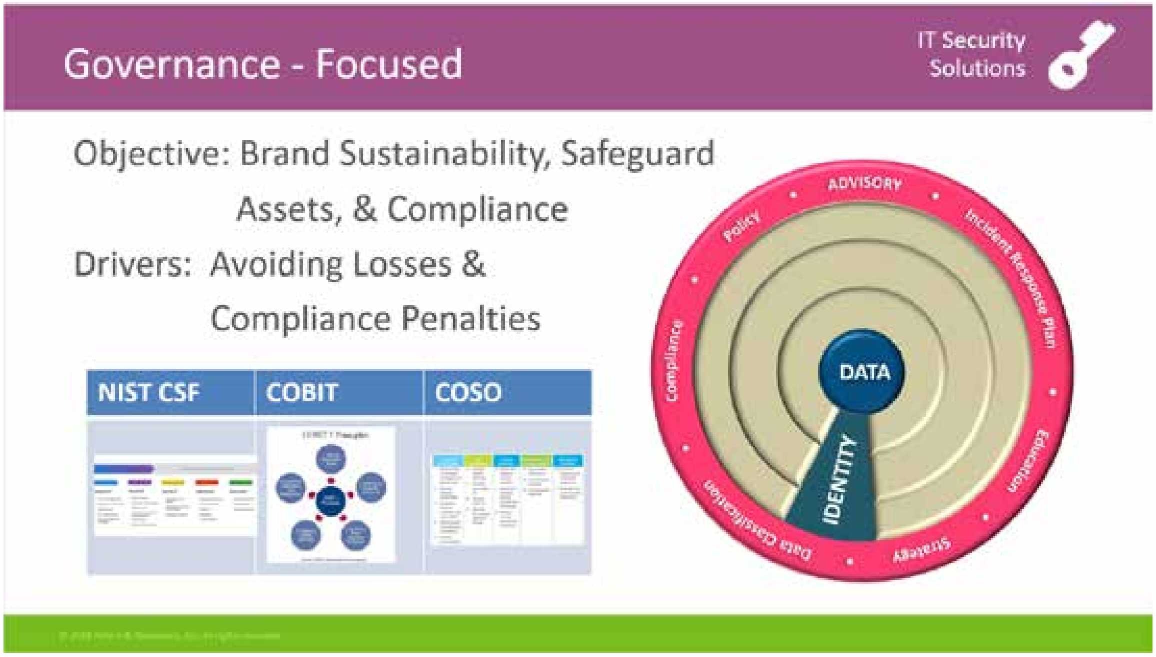
According to Infosecurity Magazine, 80% of organizations in 2015 experienced an internal security incident, and a Kaspersky article noted 60% of organizations found their ability to function severely hampered after a breach. In 2016, Data breaches spiked at by 86% with almost 1.4 billion records compromised vs. 740 Million records in the prior year according to the Washington Times. This same article, noted hackers, cybercriminals and other malicious outsiders were responsible for just over two-thirds of last year’s data breaches, while accidental loss and insider threats were ranked second and third respectively. “Knowing exactly where their data resides and who has access to it will help enterprises outline security strategies based on data categories that make the most sense for their organizations. Encryption and authentication are no longer ‘best practices’ but necessities.” said Jason Hart Vice President and Chief Technology Officer for Data Protection. Thus:

- Information Technology is increasing in complexity and changing dynamically, limiting effectiveness and efficiency of the traditional fortress defense strategy.
- Regulations and enforcement continue to increase both strain on operational budgets and reputational risk to organizations.

- There is significant need for education in organizations about leading cyber security practices for end user and information technology professionals.
- The demand for security skills is driving costs upward, therefore making it difficult to retain people skilled in information technology and cyber security. This is especially true for middle market companies. To provide some context, The Daily Dot outlines the median salary for common cybersecurity job titles:
  - Chief Information Security Officer - $195,620
  - Information Security Director - $156,230
  - Data Security Director - $143,394
  - Cross-Platform Security Manager - $129,612
  - Data Warehouse Information Security Manager - $124,125

Clearly, today's security landscape has strained the people, budgets and risk tolerance limits within organizations. To address this, forward-thinking organizations are adopting modern security models with *prioritization* and *business alignment* as cornerstones. Let's take a deeper look at three ways organizations are approaching data security today, and evaluate them to identify an optimal strategy:

1) **Governance:** Some organizations choose to focus on meeting compliance objectives; a check box approach to compliance will not be effective as all entities are not alike.

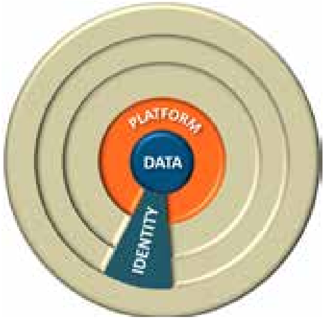


Governance - Focused

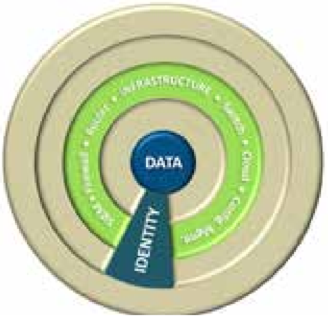
Objective: Brand Sustainability, Safeguard Assets, & Compliance

Drivers: Avoiding Losses & Compliance Penalties

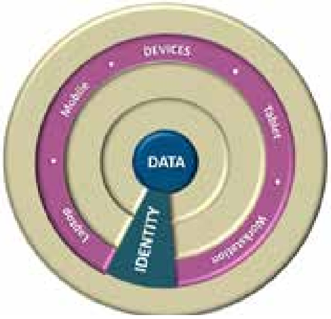
Controls / Technology: Organizations without compliance objectives most often emphasize technical controls to resolve security challenges. Graphically, this means they surround their data with layers of controls in an organized, but not in a prioritized, fashion. While this is somewhat effective when aligned with Governance, without prioritizing, an organization may risk missing protecting significant data. Thus, improper (too much or too little) emphasis is placed on data due to lack of understanding of importance such as: third-parties, development/quality assurance environments, big data or as simple as wasting time shredding Freedom of Information Act (FOIA) documents.



Platform (OS, Hypervisor)

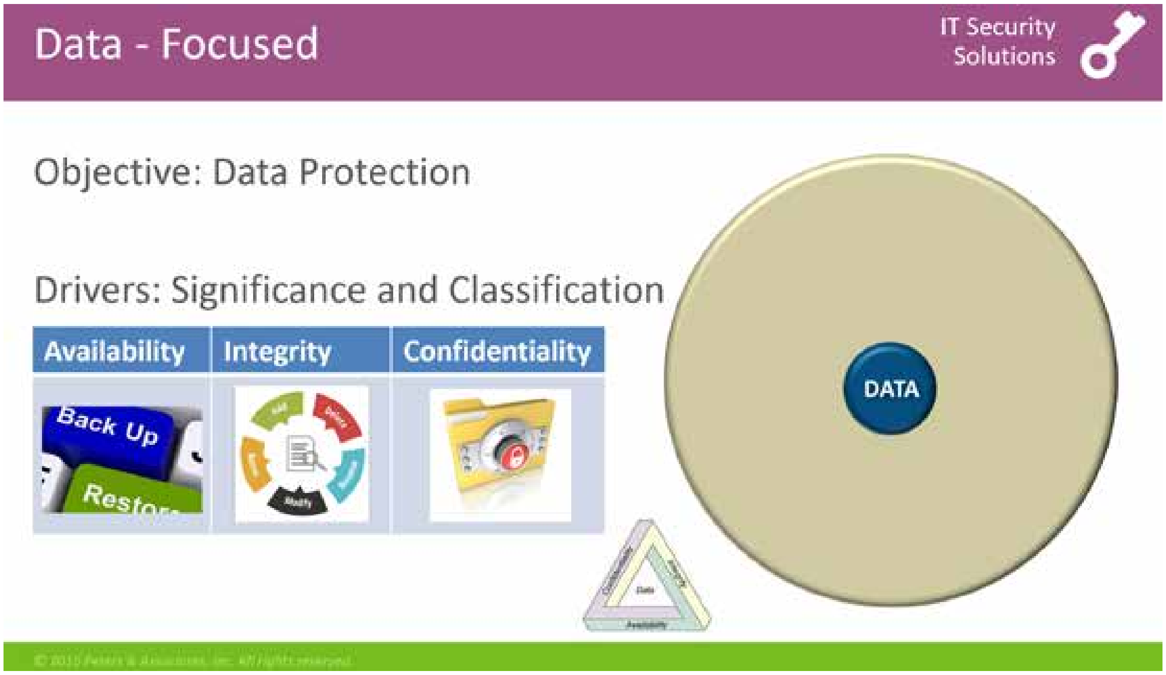


Infrastructure (Firewall, Server)



Endpoints (Laptops, Phones)

2) **Data Significance:** Organizations evaluate the value of their data relative to other data (prioritization) and on the security investment (overall control sets) to create a roadmap. It is well understood that organizations that make data-based decisions have better profitability and productivity. Therefore, it is reasonable to conclude using this methodology coupled with the right mix of governance and prioritized technology controls will produce the best results over time vs. governance and technology controls approaches alone.



Data - Focused

IT Security Solutions

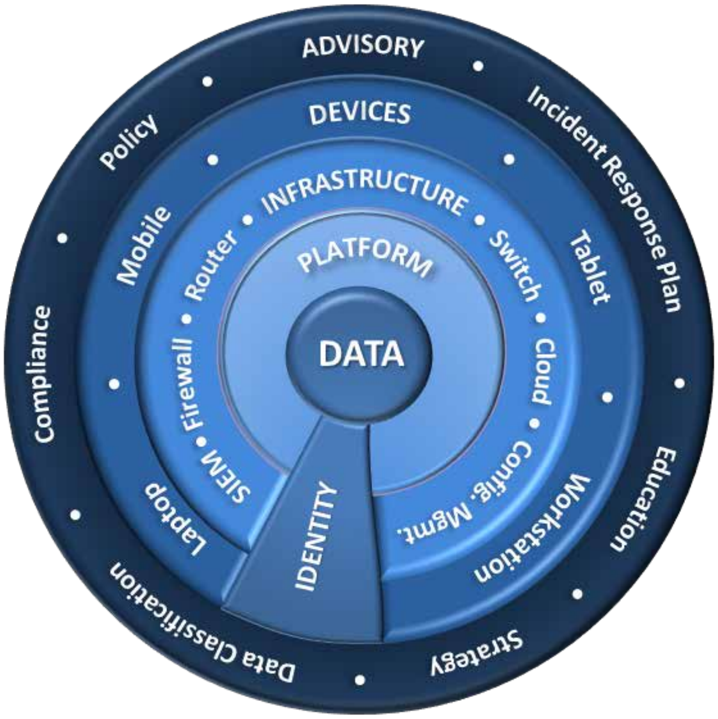
Objective: Data Protection

Drivers: Significance and Classification

Availability	Integrity	Confidentiality

© 2015 Peters & Associates, Inc. All rights reserved.

To stay ahead of cybercriminals and other risks, security strategy must be continuously, but pragmatically, re-evaluated with a risk-based approach that prioritizes using a data-centric strategy focused on resilience. The goal is to find the correct strategy, process, and technology mix for your organization. When executing this, organizations should take a holistic data-significance approach (see below) to govern security, and ensure they find more effective ways to manage business and operational risk. This approach addresses governance, and technology controls in a prioritized fashion ensuring the optimal prioritization with the organizations goals objectives, and data risks. A holistic data-centric approach needs to include the complete picture, in contrast to historical or traditional technical or compliance based controls. So, what should this look like? The following should be components of your optimal Organizational Security Strategy:



What are the next steps?

1) Establish and select an advisor for a security governance program familiar with these approaches to customize the right approach for your organization
2) Analyze strategic plans relative to their impact on entities, jurisdictions, third parties, units, functions, devices, infrastructure, and platforms
3) Inventory and classify data based on both sensitivity and criticality
4) Establish a security maturity model and design approaches that align business objectives, data requirements, and information flows
5) Optimize processes to baseline measurements for education, monitoring, detection, and incident response

Timothy O'Hara, CPA, CGMA has 20 plus years in the industry and currently an advisor with Peters & Associates. In this role, Tim supports clients in banking, healthcare, manufacturing, business services, and government in solving problems impacting business decisions and measurements supported by data in cyber-security, business intelligence, infrastructure and collaboration activities. Tim can be reached at timothy.ohara@peters.com.

© Peters & Associates. This is an article from the Governance Issues™ Newsletter, Volume 2017, Number 2, published on August 4, 2017. Use of the newsletter article constitutes acceptance of our Disclaimer and Privacy Policy.