NEXTLABS®

White Paper

The Biggest Gap in Your Cyber Security Solution

Is Your Data Protected?

Everyone agrees threats to cyber security are on the rise. But how well do organizations understand which threats they should worry the most about? Or what the biggest business impacts are? Or where the most relevant vulnerabilities tend to be?

This white paper describes the most common—and most commonly overlooked—source of cyber breach and the challenges that occur when organizations try to implement a comprehensive solution to address it.

IT Leaders, Security Professionals, and Compliance Officers will understand several challenges of addressing today's cyber security threats, as well as why the industry is currently shifting toward a more data-centric perspective.

INTRODUCTION

Cyber security threats are on the rise, presenting an ever-evolving challenge to IT organizations. But some types of threats garner more attention than others, especially viruses, malware, and external attacks. It is a mistake to think of cyber security as only a matter of protecting your internal networks, infrastructure, and devices from external threats. Countless episodes of data loss and spill from the inside, most recently Edward Snowden, teach us this.

Organizations must not ignore what has been documented as the statistically largest source of cyber breach: information shared by authorized users during normal, daily operations. In fact, what this white paper refers to as "business as usual" data handling—the access and sharing of data by well-intentioned, but potentially negligent users—poses a far bigger threat than theft and malicious attack from insiders or outsiders.

“Business as usual” breach is increasing exponentially because, across industries, business process is growing more complex. Information is being shared more broadly, across global partnerships and supply chains. Users require access to sensitive data on more devices, and increasingly, beyond the traditional perimeter of IT control and visibility. What Forrester calls the “Extended Enterprise” has become the new normal. The result is authorized, but potentially negligent or uninformed users sharing more information more broadly than ever before.

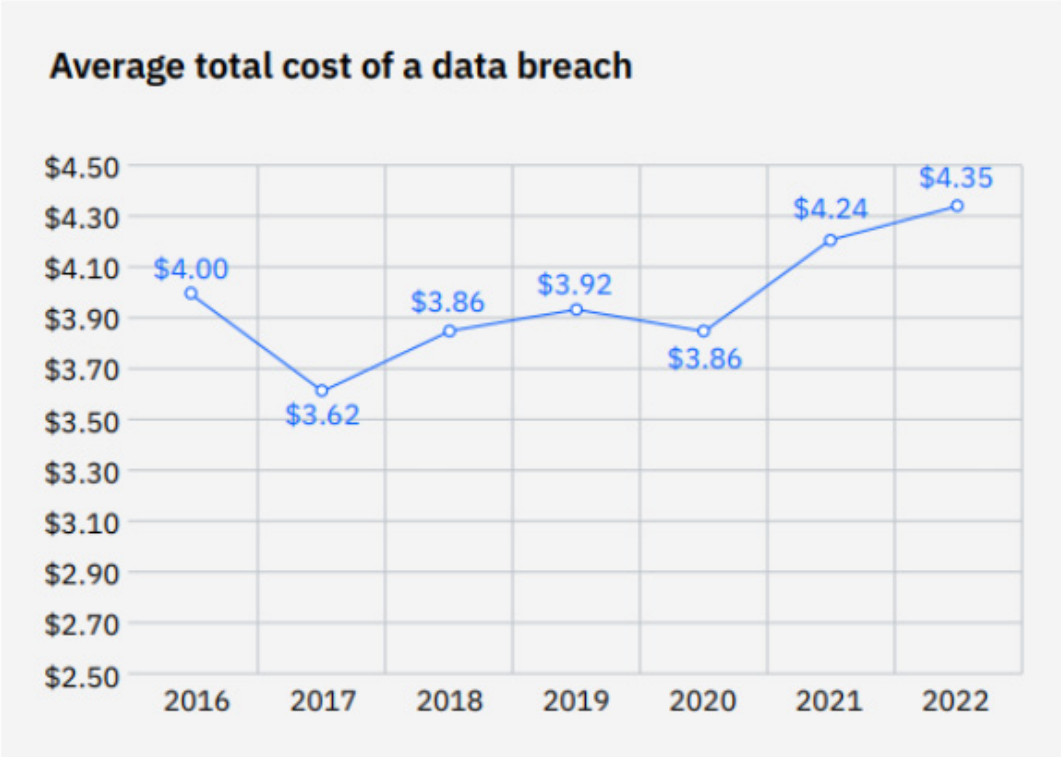
Given these trends, this white paper describes the difficulty of addressing what is probably the biggest weakness in your cyber security solution: protecting your data. Increasingly, protecting data requires organizations to target and manage data vulnerabilities directly, rather than deal with the problem the traditional way—as a matter of securing infrastructure.

Why the Rise?

To be more precise about what it means when we hear “cyber threats are on the rise,” organizations should understand what exactly is increasing. What are the trends in terms of direct business impacts? Which industries are hardest hit? What are currently perceived as the biggest sources of risk?

What is the biggest business impact...?

Organizations consistently report that the cost of cyber breach increases every year (Source: Statista, 2022). When we talk about the rise of cyber threats, it’s data loss that is on the rise, as seen in the increase in average cost of data breach, hitting a record high from 2016 to 2022. (Source: IBM Cost of a Data Breach Report, 2022)



What industries are hardest hit...?

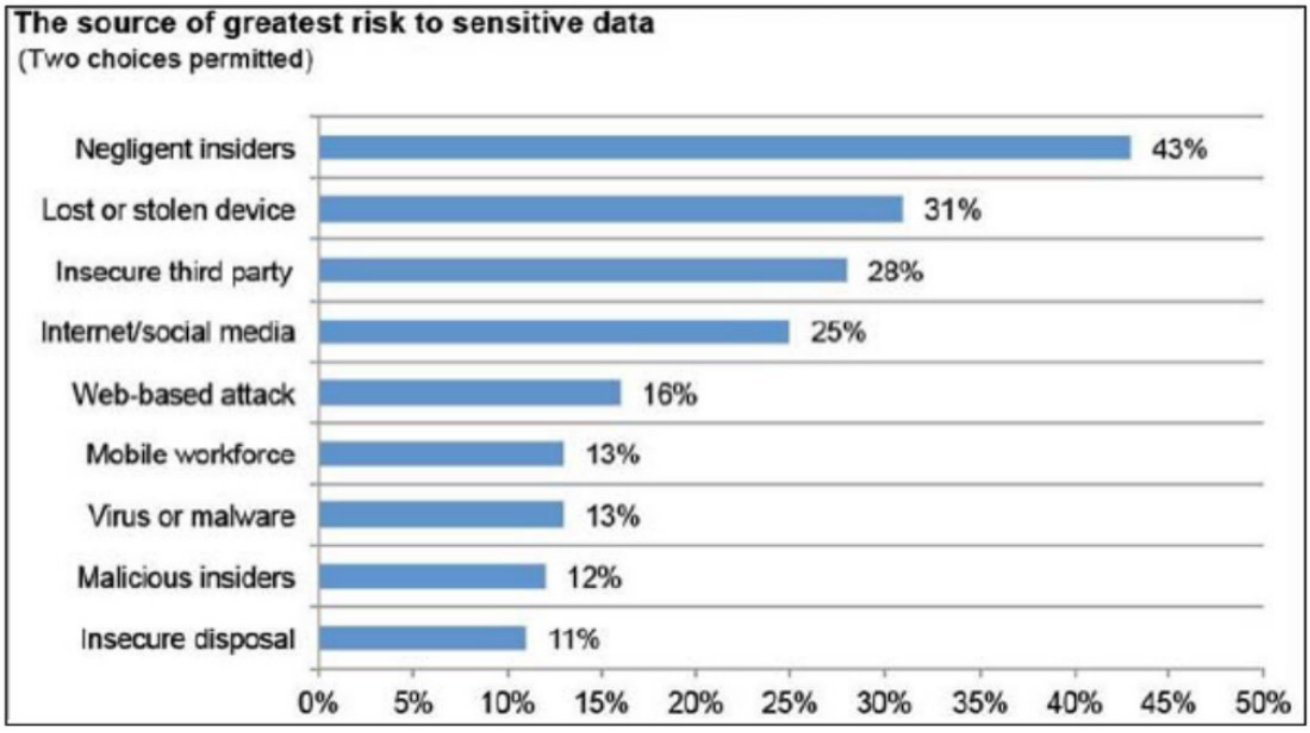
The industries reporting the highest rates of cyber breach tend to be those handling sensitive information on a regular basis. For instance, healthcare currently holds the highest spot, with an increase in total breach cost from USD 9.23 million in 2021 to USD 10.10 million in 2022). Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government. Its database consists of shared information between healthcare providers and when breached, would compromise sensitive information of millions of people.

Industry	Average cost of a data breach (USD millions)
Healthcare	$10.10
Financial	$5.96
Pharmaceuticals	$5.01
Technology	$4.97
Energy	$4.72

Source: IBM Cost of a Data Breach Report, 2022

What are the biggest sources of risk...?

Comparing different sources of risk reveals that external attacks and malicious insiders are minor risks compared with the far more relevant risk of access by regular employees and business partners. For instance, the risk of data loss caused by malicious insiders (12 %) is far lower than risk associated with negligent insiders (43 %) and authorized, though insecure third party users (28 %). Authorized users expose data to risk in myriad ways: by simply posting data to shares and portals, emailing it to partners, and losing laptops.



THE PROBLEM WITH TRADITIONAL IT PROTECTIONS FOR "BUSINESS AS USUAL"

While the causes of cyber breach are certainly many and diverse, even a brief analysis of trends suggest that the biggest vulnerabilities lie in what trusted employees and external users (third parties, external partners) do with sensitive business data. Protections must anticipate data access and sharing that is part of "business as usual, " just as effectively as external threats or malicious insiders.

However, traditional IT protections are assumed to protect data from cyber security threats because they protect data containers—on infrastructure, devices, applications, network locations. If you apply proper controls to locations and containers, you protect the data within them, right?

Unfortunately, wrong. Information sharing trends in "business as usual" increasingly invalidate this assumption. The sections below discuss business and technical trends to explain why container- and location-based controls are inadequate.

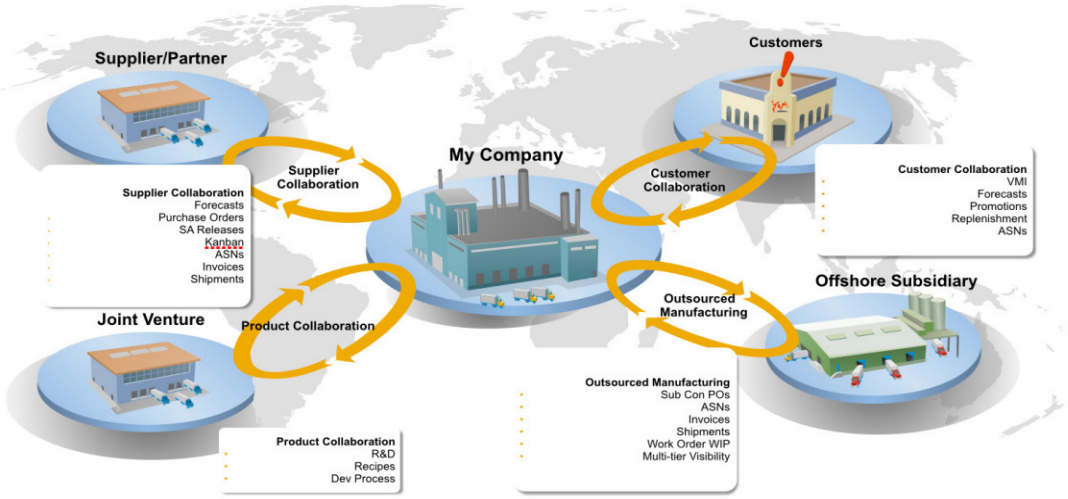
Business Trends

On the business side, joint ventures are on the rise (source: KPMG Survey on Merger & Acquisition Activity, 2013), globalized business process continues to thrive, and firms are projected to only continue in this direction: expanding their footprint to international markets to drive revenue growth. As a result, trade secrets and other sensitive data crosses organization and international borders as a matter of daily business.

The result? Information rarely stays within its "container." It moves between systems, containers, and organizations—beyond the reach of traditional IT controls.

But the answer is not to "lock data down." In many industries, adopting broader business models is a requirement to stay competitive. It is not an option to simply shut initiatives down because they introduce new forms of cyber security risk. For instance, the figure below provides an example of the type of distributed process businesses want to pursue. Suppliers/partners, joint venture collaborators, manufacturing, and customers are distributed globally, with different classes of sensitive data shared with different parties.

Securing sensitive data against cyber breach in such a case would require protecting more than just devices and infrastructure within a central company. The real challenge is protecting data as it moves between entities.



Technology Trends

On the technology side, firms increasingly need to support data access anytime, anywhere, and through any device. Ubiquitous access is such a common expectation (including among customers and partners) that, again, not embracing this trend is not an option.

Anytime, anywhere, any device access is game-changing for several reasons. Because data must be always-available, systems that support always-on connectivity (cloud storage, wifi hotspots, vpn) increase the window of opportunities for cyber breach.

In addition, with the emphasis on availability, newer mobile apps and operating systems are tailored for convenient access, more so than robust access control. This increases the already largest source of risk to cyber security—authorized users accessing and sharing data in negligent ways. Thanks to more convenient methods of access, they now do so more easily and faster than ever.

Top Three Cybersecurity Game Changers

Game Changer	Attributes	Impact
Always-on Connectivity	• Critical data and information are clustered in clouds. • Wi-Fi hotspots are growing. • Work systems are easily accessed at home or on the go.	Increases window of opportunity for attack
IT-centric Business and Society	• Online systems are the new critical infrastructures. • Society's reliance on "always-on" creates wider windows of attack time. • There is no paper fallback in emergencies.	Increases number of business processes that can be targeted
New Class System by Technology Skills	• Mobile device features remain a mystery to many. • Fewer digital natives have deep IT skills. • New apps and operating systems favor convenience over user control.	Increases role of human error in enabling cybercrime

COMPREHENSIVE SOLUTION FRAMEWORKS

Any cyber security solution will typically include hundreds if not thousands of moving parts, including different technical tools, teams, and processes. Recognizing this complexity, several standards organizations offer frameworks that provide a top-down, comprehensive view of the critical functions.

For example, the National Institute of Standards and Technology (NIST) framework organizes a comprehensive cyber security solution into the functions of Identify, Protect, Detect, Respond, and Recover (source: Improving Critical Infrastructure Cybersecurity, Executive Order 13636, NIST, 2013). Each function is further broken down into process categories, and these process categories would have to be broken down further upon implementation across teams, locations, and infrastructure.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Implementation Challenges

Frameworks like NIST are especially useful for understanding problem areas when organizations attempt to implement cyber security solutions. Challenges occur due to many factors, including (but not limited to) gaps in how traditional IT tools define the scope of a critical function, dis-coordination when functions are shared cross-teams, and “translation” of the outputs from one function to another. This section pinpoints four specific challenges that arise because of one or more of these issues.

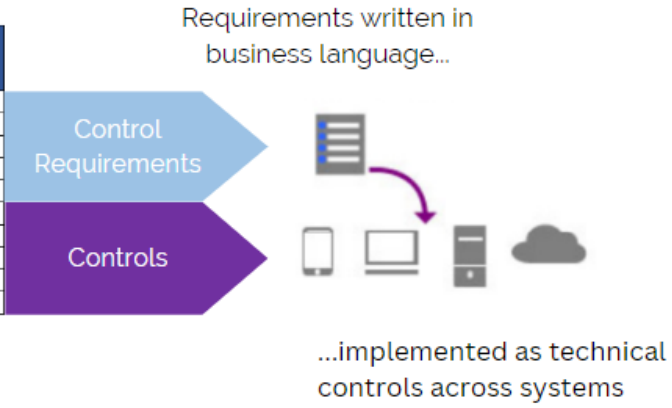
Challenge: From Risk—> to Requirement —> to Technical Control

During the solution requirements stage (in the NIST framework, within the Identify function) a team performs some manner of risk assessment to identify threats and vulnerabilities. Ideally, these vulnerabilities are mapped systematically to control requirements (the output of the Identify function). Then, other technical teams are tasked with “translating” requirements into different technical controls (within the Protect function).

The step of translating non-digital requirements into technical controls cross-system can become an implementation and maintenance nightmare, adding a significant layer of labor and the potential for human error. Technical rules must be expressed in the logic of several systems, which are typically managed by different teams.

Plus, as business process becomes more distributed and global, organizations must contend with how requirements will be translated externally, that is, by outside parties, across unknown or uncontrolled devices and applications.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology



Challenge: Inconsistent Protections

When it comes time to implement protections, controls typically target one level of infrastructure only. Each team will perceive and address threats at the infrastructure level they are equipped to deal with.

Challenge:
Have vulnerabilities been addressed at the relevant layers of infrastructure?

When one team is focused on addressing threats at the network-level, another team on device and trust, and another on securing containers in different applications (SharePoint and collaboration portals, Document Management Systems, and Line of Business applications, the resulting solution is often incomplete and inconsistent.

Implementing a comprehensive cyber security solution requires designers to include the dimension of infrastructure depth in their framework, and then assess vulnerabilities that occur at each layer.

Challenge: Centralized Visibility

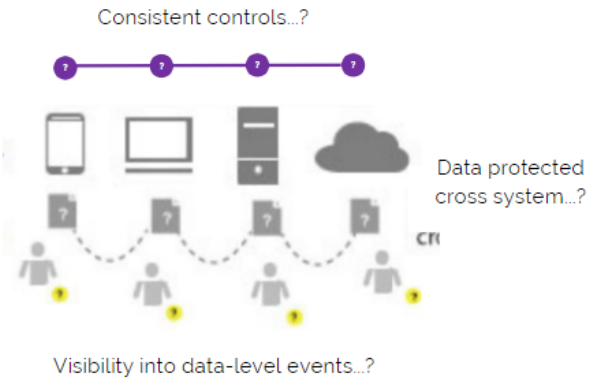
Because different teams are applying controls at different layers of infrastructure, usually using different toolsets, organizations have little to no visibility into the comprehensive picture.

Challenge:
What level of visibility do you maintain, and for what levels of infrastructure?

While it may not be necessary to apply controls at every infrastructure level, there should be at least coordination and visibility as to which levels are targeted by which teams.

This challenge is inherent in the Detect function of the NIST framework—which is typically implemented by IT organizations in terms of SIEM, Virus and Malware Scanning, and Intrusion Prevention and Detection—in other words, at the network and device layer. Visibility into application and data access across different applications is not as commonly included within the Detect function, and the result is a lack of coordinated, centralized visibility for data access events.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes

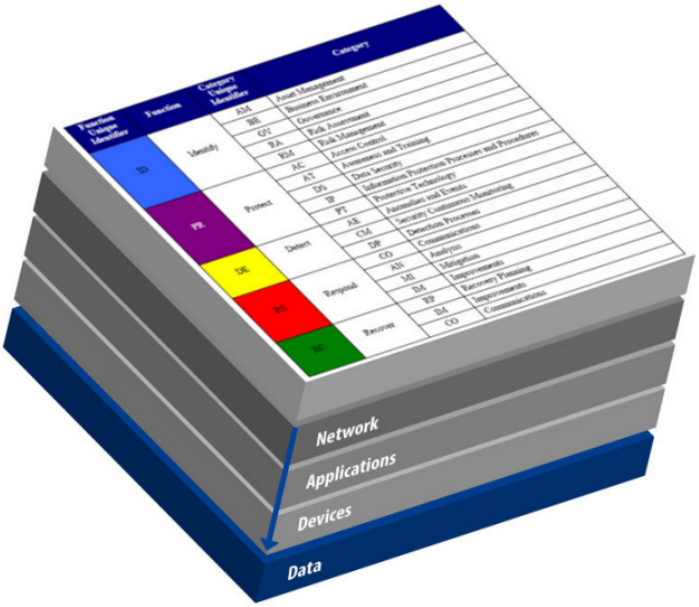


Challenge: The Data Level

The last challenge actually underlies all the other previously discussed: the failure of cyber security solutions to extend all critical functions down to the data level.

Even though the need to protect data may (or may not) have driven requirements definition at the Identify stage, available IT technologies will implement controls based on container, Access Control List (ACL), Security Group, and Permissions. In translation to the “Protect” stage, data is protected indirectly—and the explicit focus on data vulnerabilities is lost.

Plus, when controls are inconsistent across systems and levels of infrastructure, data is not protected while on-the-move in the course of daily business. And while there are myriad event monitoring tools that detect events at an infrastructure or container layer, there is no comparable level of visibility into data access, usage, and sharing events.



AN INEVITABLE SHIFT

The shift to data-centric protection is inevitable, as acknowledged by industry analysts like Forrester and Gartner. As discussed above, the primary goal of a cyber security solution is to prevent data loss—the biggest pain point of cyber breach. However, implementation process often obscures this primary goal.

Today, sizable IT investment is already tied up in traditional infrastructure-centric security and team competencies. Plus, organizations typically do not have the right kind of data-level awareness into where data moves during “business as usual.” This awareness is absolutely critical for identifying vulnerabilities at the data layer, and should be the real starting point of any solution design.

This data-centric perspective would need to be developed while IT still continues the standard work of reinforcing network perimeters, maintaining lists of trusted users and devices, and applying application-centric, container-based controls. However, the benefits of making the shift toward data-centric thinking promises to be well worth the effort. Protecting data directly, rather than just securing infrastructure, can result in data being protected from cyber breach no matter where it is stored, who is accessing it, or how it is being consumed or distributed.

Information Risk Management

One thing is clear: as organizations re-orient their controls, processes, and mind sets around the data layer, the work of implementing frameworks like the NIST standard will change. The focus will shift from the current business of "translating" requirements into technical controls, to identifying risks and vulnerabilities specific to data, then mapping data-centric vulnerabilities down to system- and application-level controls.

The next white paper in this series, "Information Risk Management: Cyber Security at the Data Layer," describes how to design cyber security solutions around business requirements, rather than infrastructure.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.