TEKsystems
Own change

DATA SECURITY:

The Race to Optimal Performance and Protection

CONTENTS

WHERE DATA AND SECURITY PERSPECTIVES MEET

DATA AND CYBERSECURITY EXPERTS DISCUSS PROTECTING THE MOST VALUABLE ASSET: DATA.

Bringing their unique perspectives as architects of data solutions and cybersecurity solutions, TEKsystems experts sat down to discuss key challenges enterprises face when it comes to cybersecurity—bringing a holistic view to the technology, process and people factors behind data integrity, availability and security.

The Security Perspective

Mike Mulligan (MM)

Director, Risk & Security

Security executive Mike Mulligan has been in the tech industry for nearly 25 years and has vast experience overseeing market development and revenue growth strategies. In his current role, Mike oversees a growth-oriented segment focused on helping customers solve technology and business challenges within cybersecurity and risk areas. Prior to his current role, Mike worked in a variety of capacities at TEKsystems, starting as a technical recruiter, then growing into roles including senior account executive, where he was highly successful in solving customer problems for Fortune 100 customers in financial services, insurance and pharmaceutical verticals. Mike has held many sales leadership and product executive roles with a primary and maniacal focus on increasing revenues and expanding market share.

The Data Perspective

Srinivasan "Srini" Swaminatha (SS)

Managing Director, Modern Cloud Analytics

Srinivasan "Srini" Swaminatha has been helping customers realize the true value of their data with TEKsystems for 12 years. Having worked with data analytics and development throughout the last 20 years of his career, Srini uses tech advancements to navigate the constantly changing landscapes of advanced analytics and business intelligence.

1 THE EVOLVING LANDSCAPE

The Growing Value of Data and Vulnerability of Data Breaches

DATA HAS BECOME THE MOST IMPORTANT ASSET FOR AN ENTERPRISE

UNLOCKING ITS VALUE LEADS TO:

- More informed, agile business decisions
- New revenue streams
- Opportunities to monetize data
- Progress through shared insights in the field

> **MM:** *"Ten years ago, we didn't talk about data that much. We used it, but we didn't talk about it empowering organizations, opening new markets or as a value stream or financial stream. It was just something we used, right? There's been this explosion in how we use it."*
>
> **SS:** *"Even 'data is the new oil' has become four or five years old now. Customers have so much data, and they want to monetize it."*

Data exists across functions within an organization—often accessible to many. But who is governing and protecting that data? As threats emerge, expand and evolve, successful leaders must view safeguarding their company and customer data as a nonnegotiable business priority.

DATA BREACHES ARE COMMON AND COSTLY

A 2021 IDC survey found more than one in three organizations globally experienced a ransomware attack or breach in the past year.[1] A cursory look at data breaches in recent years reveals multimillion-dollar losses. But there are other long-term consequences as well: losing customers' trust and damage to brand reputation.

WHO OWNS DATA SECURITY?

> **MM:** *"Who owns application development? The app dev team. Who owns the network? The networking team.* ***But who owns the data****? That can be different for each company. It may be six different people. There's not a single home for data. It's a common problem across companies and industries because how we use and manage data is very different."*

Data is a shared asset. Securing it is a shared responsibility. In theory. But what does that look like as business and IT leaders grapple with silos, budgets and massive shifts in the workforce?

2 TECHNOLOGY

Balancing Speed and Security

BALANCING SPEED AND SECURITY

> ***SS:*** *"When working with customers, bottom line, we always start by asking, 'What is the business problem?'"*

The follow-up: "How can we solve that business problem with security, flexibility and performance in mind?"

> ***MM:*** *"At the end of the day, company leaders understand they have to stay ahead of the latest threats. But we all want to focus on growing business, empowering our workforce and delivering value to customers. So, we bring it back to:* ***How can security enable the business****?"*
>
> ***SS:*** *"We are seeing all kinds of complex use cases for data;* ***security is key. But how to achieve it without slowing things down? That's important****."*

New technology drives organizations to move at the speed of their ambition. But many can face major slowdowns by only thinking about security in the final hour.

> ***MM:*** *"Many organizations are stuck in the process where they end up trying to secure something after they build it.* ***Why don't we plan on security right from the onset?*** *We'll get something* ***more secure and more agile****."*

Foster a security culture. Solving business problems with a security-first approach better protects your data and future-proofs your business.

THINK DATA, SECURITY AND DIGITAL TRANSFORMATION (DX)

Data can power an organization's digital transformation, but can investing in DX also improve data security? Research suggests, yes.

Technology Benefits Achieved from DX

37%	Analytics and Business Intelligence Reporting
35%	Predictive Analytics
34%	Security
29%	Data Privacy
20%	Control over Data Location (i.e., state or country)

Top DX Goals

23%

Bolstering cybersecurity

Top DX Challenges

24%

Security concerns and compliance constraints

With roughly the same proportion of company leaders identifying cybersecurity as a top goal and an obstacle in their digital transformation efforts, one truth emerges: security cannot be an afterthought. And yet, IDC's 2021 ransomware study revealed that organizations further along in their multiyear DX plans were less likely to have suffered a ransomware attack.[1]

What's the relationship here? The most successful DX efforts come from aligning business and IT leaders early in the process. It's likely that communication between business and IT stakeholders is the key to growth and resilience for your business and security posture.

Build alignment between business, IT and security leaders to see the whole picture and get buy-in on big initiatives.

GO FOR THE GOLD (ZONE)

How can advancements in technology secure data so that the right people get the right access to it? One solution? The gold zone.

Data lakes allow data to be segmented into zones with different use cases, access and governance standards. Commonly divided into three or four separate zones, data lakes are organized by how the data is refined.

> ***SS:*** *"Most of my work with data involves ingestion, processing and consumption. In modern cloud data warehouses or data lakes, we have bronze, silver and gold zones. We are defining that robust gold zone and embedding security to guarantee that **you can rely on business decisions made from data in that gold zone**."*

Define your gold zone with security and governance.

MODERNIZE WITH MICROSERVICES

Organizations have uncovered a newfound agility with a microservices architecture. The bonus? Better opportunities for securing data so that the right people access it at the right time.

> ***SS:*** *"Most of our customers are moving into a microservices-driven architecture, so there is—if not real-time—near real-time processing, moving data through different channels. We are seeing **data travel encrypted and only decrypted at runtime** when it is about to be displayed."*

Use microservices architectures and containerization for improved agility and security.

MIND THE GAP: LEGACY TECHNOLOGY IMPEDES PERFORMANCE & BUSINESS AGILITY

Organizations can use insights powered by data to adapt and meet market demand. But it starts with making sure no legacy technology is keeping you from true business agility. A modern cloud platform alone is not enough to optimize data performance and security, especially if the rest of your tech environment includes legacy IT. It's more than just a "technical" problem—it's a business problem.

> ***SS:*** *"During our customer's comprehensive data assessment, we discovered that even though at an infrastructure level their IT team had a cloud platform, they were running all their systems on a legacy data warehouse.* ***They had the horsepower, but they were running a bullock cart.*** *Use that horsepower to form a serverless architecture to avoid slowing things down."*

Confront your technical debt to improve performance and business agility while reducing risk.

Start with a wide-angle lens. Securing your data encompasses securing physical access, identity and digital access, application security and implementing a threat-hunting program to be proactive and stay resilient. If you're not looking at it all, you're missing the big picture.

FIND THE BALANCE:
EASE OF ACCESS VS. SECURITY

As organizations elevate experiences for customers and their workforce by prioritizing ease, they may be inviting breach. Ease of access can make an organization an easy target.

Given how data is shared, identity is the only perimeter. Consider employees' single sign-on (SSO). A single click authenticates the user and instantly takes them to their data. But what happens if that one username and password has been compromised?

> ***SS:*** *"The data team comes in to prepare the lineage, governance and boundaries. And there are resources to identify compromised credentials. For sensitive data being accessed, a microservices application programming interface (API) gives you real-time check: does this user fall under the compromised user list? You don't have to change your data ingestion patterns or storage patterns, but you need to* ***start putting wrappers around your sensitive data sets****. Use second-level verification to ensure a compromised username and password doesn't wreak havoc in your ecosystem."*

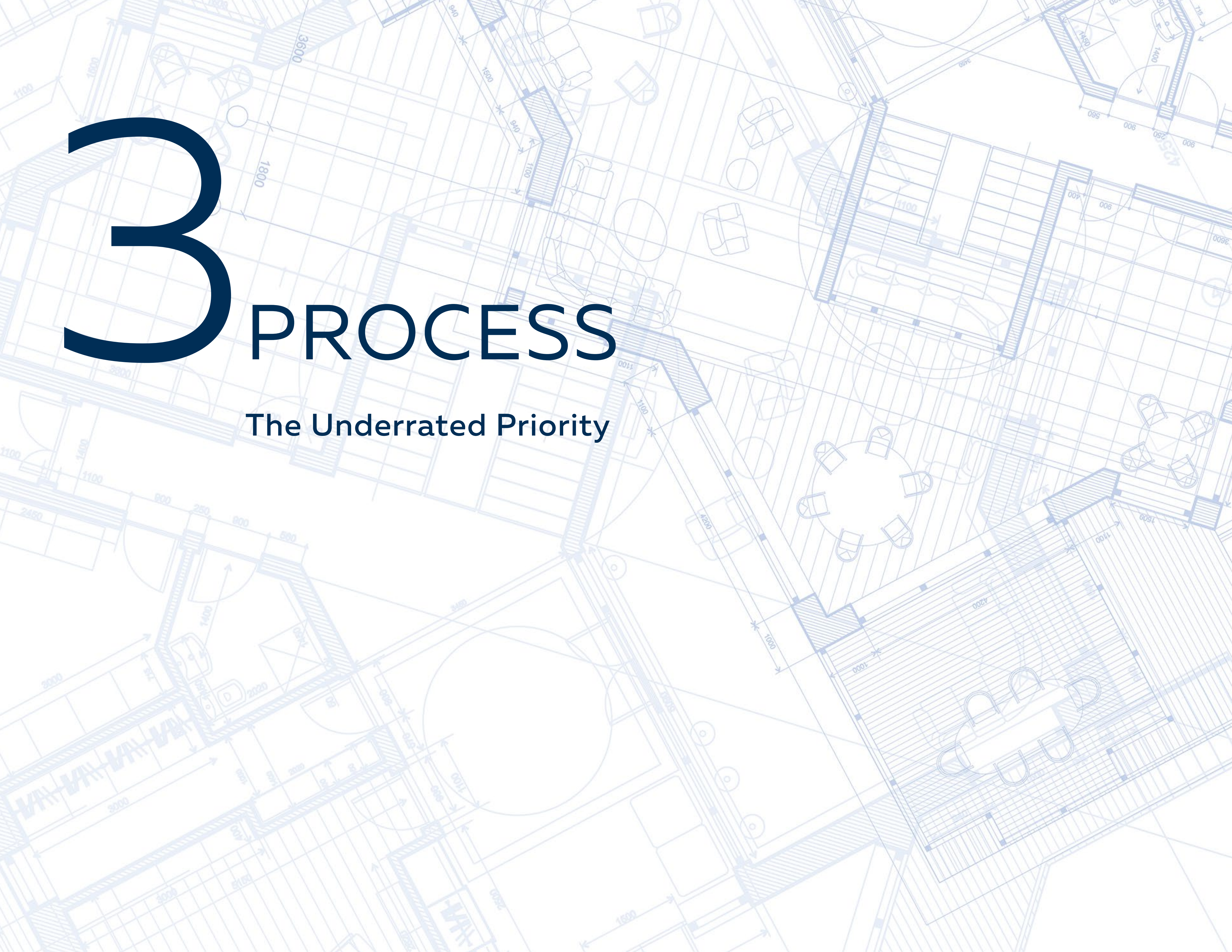
Beyond the challenges of accessing and sharing data within an organization, securely sharing data with external partners can be more complex. Organizations may engage trusted partners to meet customer needs quickly and seamlessly. Secure Data Exchange (SDE) can help organizations address privacy and compliance concerns when securely sharing sensitive data.

Protect your data with a super suit. Microservices APIs and policy-based access control act as wrappers to protect your most sensitive data, for security without sacrificing speed.

Share data securely by implementing Secure Data Exchange and segmenting any third-party data in your environment to reduce your risk.

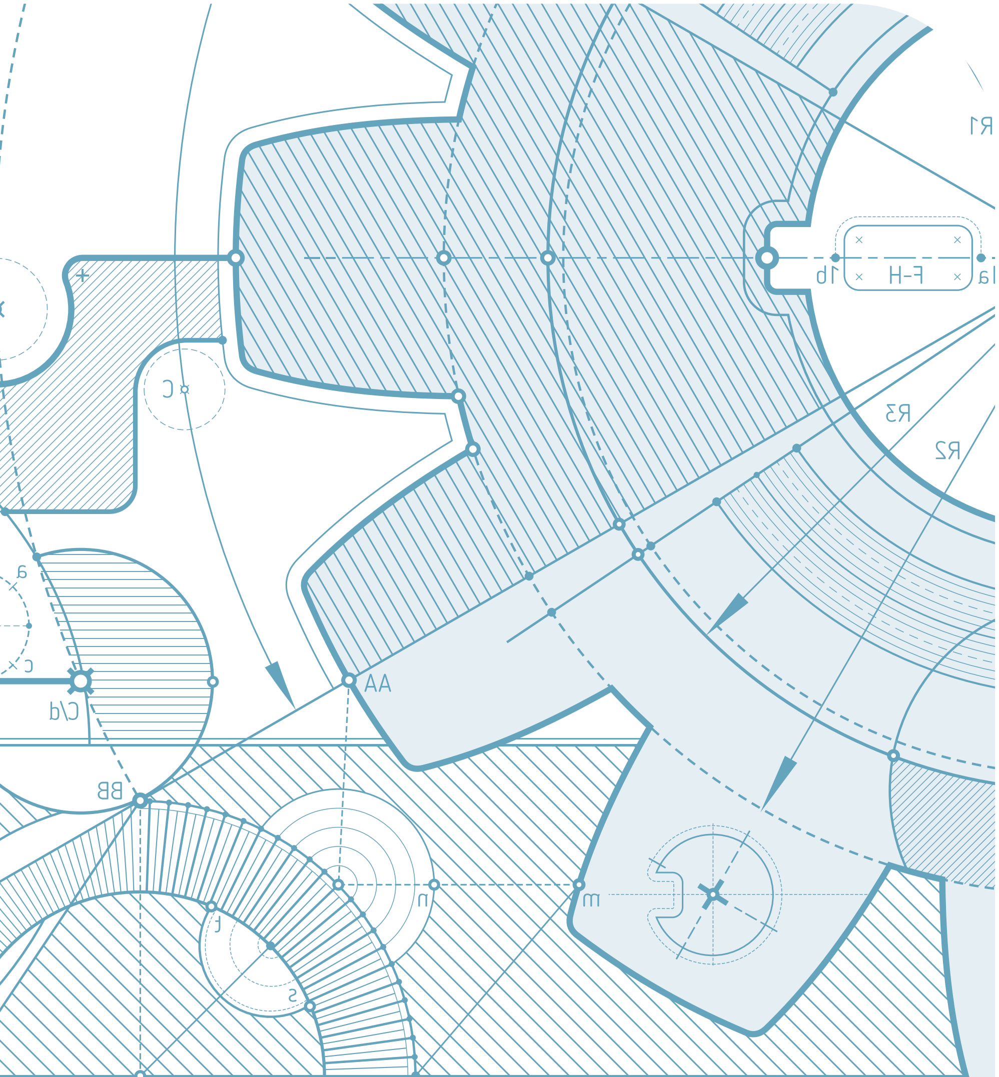
3 PROCESS

The Underrated Priority



Looking at technology, process and people, process is often treated as a footnote. The culprits:

- Ambiguity around who has visibility and power to address process
- Difficulty demonstrating ROI
- Less definitive budget for process
- Lack of visibility between functional teams



No single security tool or new team member will solve data security problems. Companies must also look to governance. Not only database governance to ensure data integrity but also security governance—systems, frameworks and processes that:

- Keep assets and operations secure
- Help you meet compliance standards
- Minimize possible damage in the event of a breach

REACH BEYOND ROI

Because it's easier to measure ROI and other improvements from technology investments or talent acquisitions, process gets less consideration.

> **MM:** *"**The ROI in security is the breach that doesn't happen**, the information that isn't compromised, the customer loyalty and dollars that aren't lost. It's more challenging to capture that. Process can be forgotten, generally because it's hard for a CTO to measure."*

But **what enables technology? Process**. Without process, you're not maximizing the value of technology or effectively protecting your data.

> **MM:** *"In many cases when breaches occur, it's not a matter of technology failure. More often, process—or lack of process—being followed is to blame. Think about dollars spent on monitoring systems and other software and tools. Are you getting the full value of, let's say, an early detection if you don't follow through?"*

Review your processes before buying another security tool. Without a process revamp, more spend may not add more data protection.

ALIGN MANAGERS AND C-SUITE

Reviewing and improving processes doesn't necessarily require massive spending, so why isn't it the first thing companies do to mature their security posture? Because they don't have the right people enrolled in their efforts.

> **SS:** *"With visibility into the lifespan of data, managers have more control than they imagine. Simple, process-related steps to protect access to data are critical. And **sometimes these process decisions don't need a C-level blessing.**"*

But the processes—or breakdowns within them—are best addressed at an enterprise level.

> **MM:** *"One of the challenges that we've seen is that a manager's view can be a bit siloed. We're talking to them about a specific issue or use case; when we're talking to the C-suite, it's enterprise level."*

With data as a shared asset across the enterprise, who owns data? Who owns data security?

> **MM:** *"I may be talking to an application security team, and data security or data protection is half the conversation. But they don't have budget or access into that data world. How do we get it? Who owns the data? **We can't talk about data without the infrastructure, systems and people using it. It's a holistic conversation.** But a single manager has their responsibilities and finances focused on one piece."*

Process is often not the primary discussion point in the C-suite boardroom, but it needs to be. Real, holistic processes need to be addressed at enterprise level—and that means you need more than the C-suite's awareness. You need them bought in and enrolled.

Reframe data security as an enterprise-level effort, needing enterprise-level visibility, buy-in and budget.

Enroll a consultative security services partner with the insight and bandwidth to take that holistic view of your systems and functions.

BUILD YOUR OWN DATA SECURITY FRAMEWORKS

> **MM:** *"There's no singular, universally agreed-upon approach to protecting and securing data."*

With no universally agreed-upon standard or framework like ITIL or Agile, each enterprise may have a different approach—and different stakeholders involved—when it comes to securing data throughout the data life cycle.

> **SS:** *"Think about policies around the data lifespan and how data flows. In data projects, we use a metadata-driven framework to help with scale and defining rules for data lineage. We see how data moved and was changed throughout the life cycle. That way, we can assure security to a certain extent as part of the process."*

Inject security into your business processes, operations and CI/CD pipeline.

GET PROACTIVE WITH THREAT HUNTING

How can you protect data in your operations and processes? Think security-first, security-always. Adjust to a proactive approach with a threat-hunting program.

> **MM:** *"Threat hunting is a continuous program. Think threat modeling on major steroids. We're evaluating threats, potential vulnerabilities in the application, data, infrastructure and cloud instances; it's looking at everything and it's looking at it continuously, because threats and vulnerabilities continuously change. The processes have a framework and are designed specifically for your environment."*

Enlist a security services partner to implement a threat-hunting program to both holistically evaluate threats to applications, data, cloud and infrastructure environments and build measures to secure these environments.

ASK THE RIGHT QUESTIONS: IS THE PROBLEM LEGACY TECHNOLOGY? OR LEGACY HABITS?

Technology modernization cannot guarantee improved data security without change management, adoption and training. You may no longer be held back by legacy IT, but you're being held back by legacy processes and habits.

> ***SS:*** *"After one of our customers invested millions in this high-tech, cloud-based ecosystem, people still downloaded reports into a spreadsheet and sent as email attachments. Even though that data was protected with APIs, the* ***data security disappears with legacy habits*** *like attaching the spreadsheet and sending it to anyone. Where there is sensitive data, you need to add a policy that can immediately block, hide or encrypt it under certain conditions. That has to be in your process."*

Go beyond the technology "what" to the behavior "how." Incorporate a security mindset and best practices when adopting new technology.

Examine your data security approach—technology and processes—throughout every stage of the data life cycle. For example, it may be secure as stored, but if you aren't addressing how to share it securely, you're still vulnerable.

4 PEOPLE

The Human Element

Organizations must confront the people-related security challenges to protect their data.

The human element of cybersecurity has always been the greatest weakness, but with the right security strategy, it can become the greatest asset.

85%

of breaches involved the human element.[2]

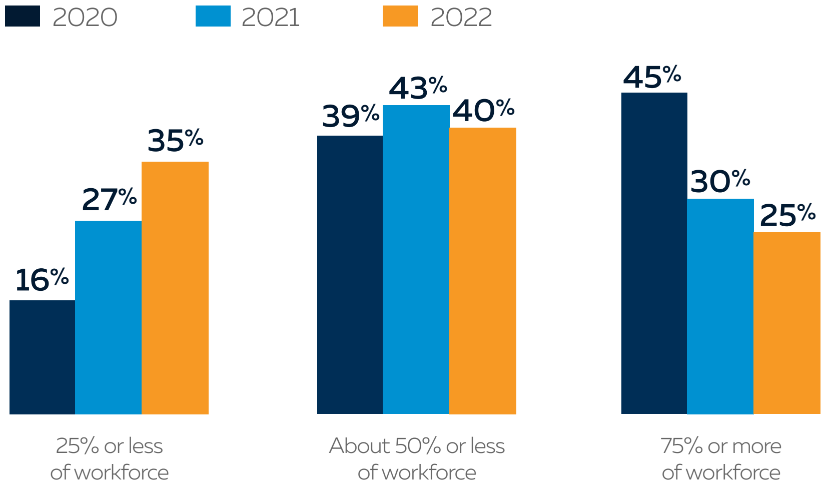
WORK-FROM-ANYWHERE MEANS SECURITY EVERYWHERE

Remote work expanded the attack surface for every organization, and security teams are still reckoning with long-term security impacts of quick decisions made to maintain business continuity in early 2020. What remains? Hybrid work models and bring-your-own-device (BYOD) policies where employees access company data and applications on personal devices and home networks.

You are at the mercy of not only your employees' tech habits but also the behavior of everyone who shares their network. Security teams that haven't adjusted are sure to face the most disruption and frustration.

REMOTE WORKFORCE EXPECTATIONS

PERCENTAGE OF WORKFORCE EXPECTED TO WORK REMOTELY



Percentage of respondents who expect that 25% or less, around 50%, or 75% or more of the workforce would work remotely three or more days per week.

Make your workforce a security asset.

1. Incentivize and reward the behavior you want.
2. Train them to use the most secure approaches to accessing or sharing data.
3. Empower them with training that will improve their tech habits both at work and at home.

Upgrade from the minimum "required cybersecurity training" to ongoing cybersecurity hygiene.

1. Use continuous education to keep your workforce prepared as threats evolve.

Make your security team a trusted resource for employees.

1. Phishing, malware and ransomware attacks work because they create panic, shame and isolation. Fight back with preparation, education and community.

CYBERSECURITY TALENT SHORTAGE & SKILLS GAP

The tech world competes for highly skilled thinkers and innovators. Outnumbered by bad actors, security teams feel the squeeze even more with more job openings than people to fill them. Reportedly impacting over half of organizations, the cybersecurity talent shortage is not disappearing anytime soon.[3] In a global survey of nearly 500 cybersecurity professionals, 95% of respondents reported the cybersecurity skills shortage and its impacts have not improved over the past few years—44% say it's getting worse.[3]

> ***MM:*** *"Cybersecurity leaders face immense pressure to protect their organization from well-funded, incredulous, savvy bad actors. Their plates are full—overflowing. Add in the tremendous shortage of talent in this space—It begins to seem like a massive undertaking."*

Bridge the gap with upskilling and reskilling.

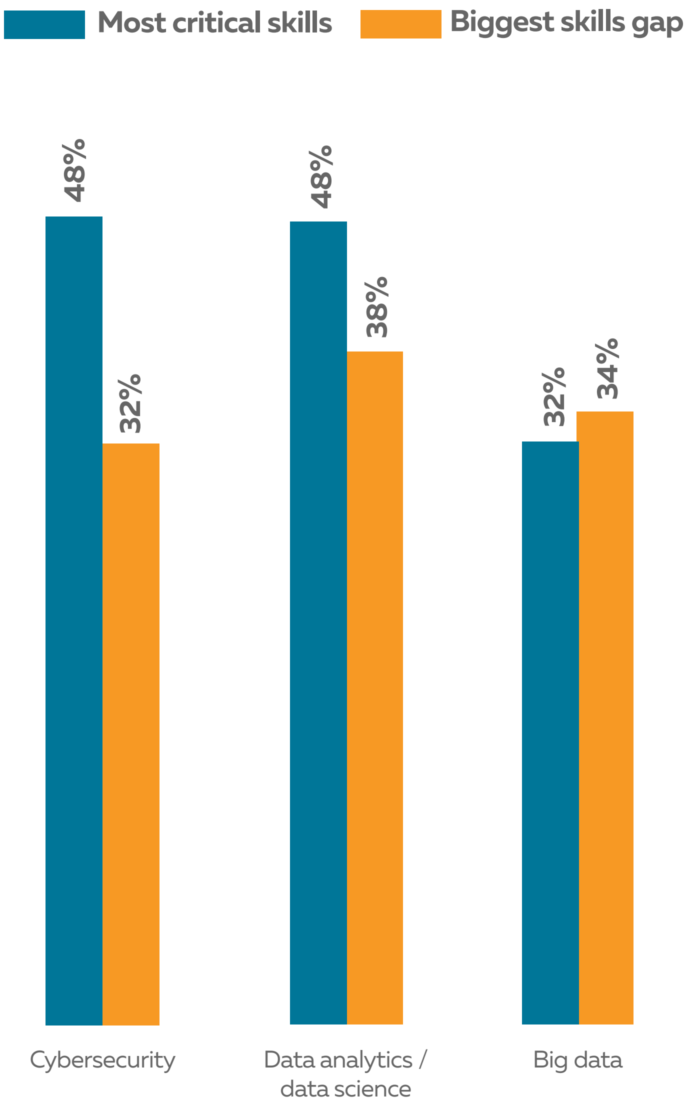
1. Invest in your people to improve resilience and avoid attrition and burnout.
2. Seek out and train strategic minds that stay flexible as technology and threats change.
3. Teach what you can teach. Hire what you can't.

Build specialized security teams.

1. Break down silos and build a shared language for better visibility, communication and collaboration across disciplines.
2. Build cross-functional teams with a wider range of skills and expertise to be more adaptable to the ever-evolving threat landscape.

Develop security champions outside the security team.

1. Imagine your application development team thinking about security as they develop, or your data team considering not just database governance for data integrity but also the governance processes to ensure data security.



THE GREAT RESIGNATION. THE GREAT RESHUFFLE. THE GREAT BIG HOLE IN YOUR DATA SECURITY POSTURE.

Over 47 million people quit their jobs in 2021.[4] With a revolving door of access to company data, it's past time to reconsider your approach to provisioning and de-provisioning employee access.

> **MM:** *"If a former employee can still log in and access company data, that unrevoked access is an opportunity for breach."*

Even for organizations that have already automated de-provisioning, the data security implications of turnover start before an employee gives notice. To stay proactive, identify behavior before termination that could signal a problem—think increases in or irregular file sharing.

Include a well-considered, holistic identity and privileged access management program in your data security strategy.

Make sure the right people have access to the right data at the right time with role-based access control and policy-based access control.

Look for holes in your automated de-provisioning access to avoid data security issues during offboarding.

Sources

1. IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach, IDC
2. 2021 Data Breach Investigations Report, Verizon
3. Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment, Information Systems Security Association International (ISSA)
4. The Great Resignation Didn't Start with the Pandemic, Harvard Business Review

TEKsystems

Own change

Experience the power of real partnership.
TEKsystems.com

Follow Us