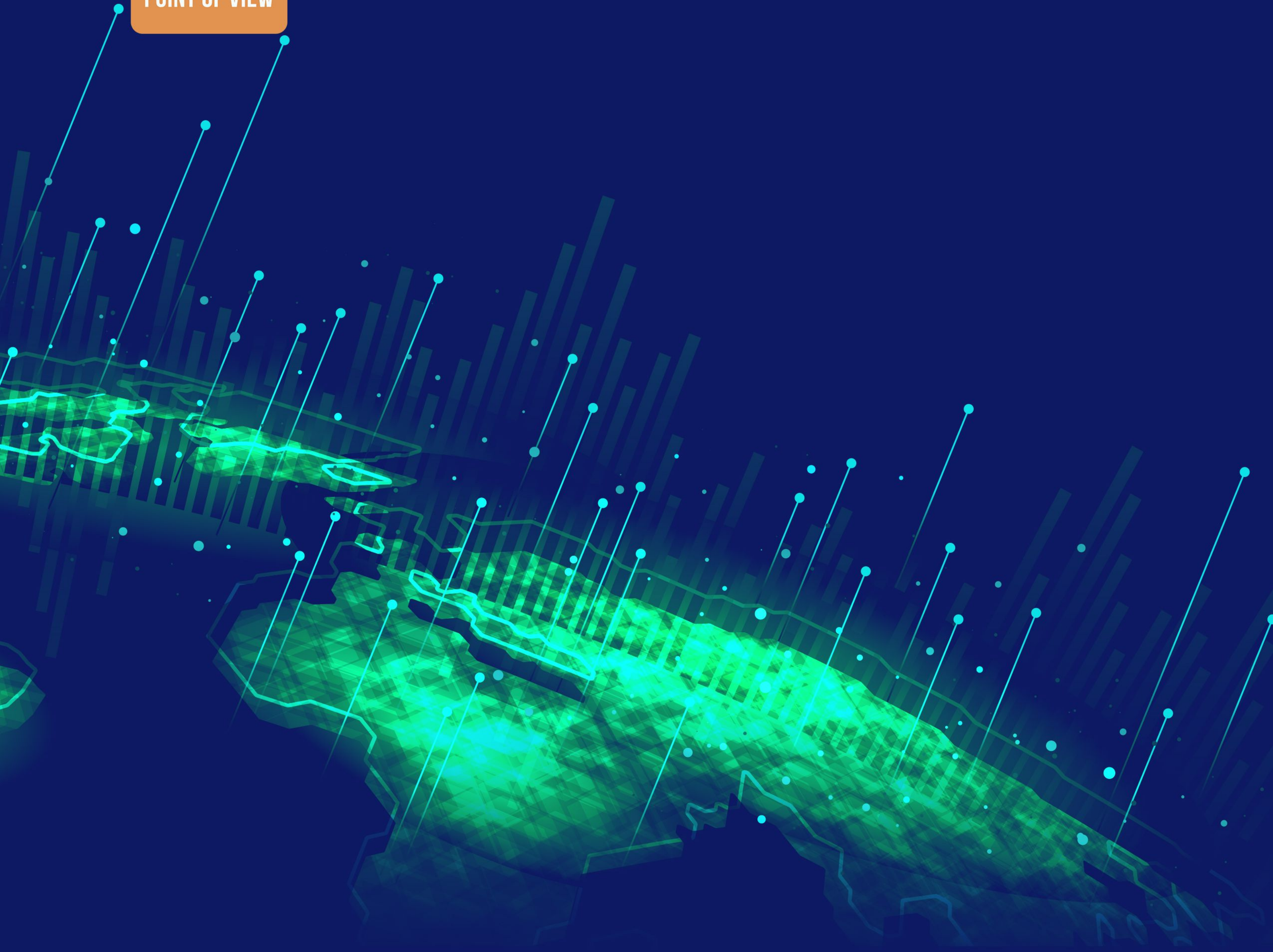
CISO
POINT OF VIEW



The ever-changing role of data, and the implications for data protection & storage security

WRITTEN BY CISOS, FOR CISOS

CONTINUITY

FOREWORD

The role of data in the modern enterprise is continually evolving. Digital transformation brings data much closer to both customers and end-users, with much larger volumes of data being captured to streamline services.

At the same time, the “[1]**business value**” of data continues to grow, making it an organization’s key – if not primary – piece of intellectual property.

From a cyber risk perspective, attacks on data are the most prominent threat to organizations. Recent years have witnessed a dramatic shift in the cyber threat landscape, with organizational data becoming a prime target for cybercriminals.

We see a year-on-year increase in the number and sophistication of data-targeted attacks, leading to near-exponential growth in cybercrime

Legal or not, any industry that demonstrates such growth will typically also exhibit significant re-investment of profits, and accelerated innovation. This means that things could get much worse, with new forms of data-targeted attacks beginning to emerge.

As repercussions of cybercrime on nations’ economies and freedoms are unfolding, regulators (domestic and international) are paying much closer attention to the responsibility that organizations have of guaranteeing the integrity, resilience, and recoverability of their data and their services.

DORON PINHAS

CTO, Continuity and Co-Author of the NIST Special Publication 800-209 ‘Security Guidelines for Storage Infrastructure’

[1] A way to quantify the significance of digital data for a given organization is to estimate how much its loss would depreciate from the total value of the business. For certain businesses (e.g., mining, manufacturing, museums), the business value is likely quite low (only a few precent). For others (e.g., digital currency companies, content creators), it could be close to 100%.

THE CISO PERSPECTIVE

We wanted to get the opinions of CISOs on the topic of securing data assets:

What contributes to the increase in data's 'business value'?

How is technology adapting to accommodate this change?

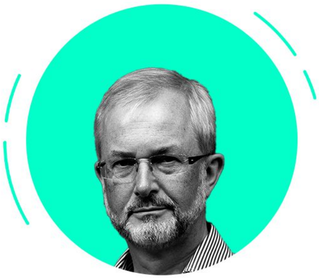
Which security practices have evolved, and do they match the current business needs?

Top recommendations for your peers

CISO lessons learned: how did you approach data protection in your career? What worked and what didn't, and what would you have done differently?

Where should other CISOs start when it comes to taking a risk-based approach to data protection and recoverability?

We interviewed the following eight seasoned CISOs and Cybersecurity leaders to get their unique insights.



John Meakin
Former CISO
GlaxoSmithKline, BP, Standard Chartered, and Deutsche Bank

Joel Fulton
Former CISO
Symantec and Splunk

Endré Jarraux Walls
CISO
Customers Bank

George Eapen
Group CIO(and former CISO)
Petrofac

Sunil Varkey
CTO (and former CISO)
Forescout Technologies

Ian Thornton-Trump
CISO
Cyjax

Ashish Thapar
VP Consulting – APAC
NTT Security

Dick Wilkinson
Former CISO
New Mexico Supreme Court

THE IMPORTANCE OF DATA IS GROWING

There's a consensus that data is quickly becoming a key asset most for organizations. **Sunil Varkey, CTO at Forescout Technologies (and former CISO), explains**, "Data is the new oil. It is core to the business since data drives every decision, trigger, campaign, and automation in our new digital world."

Over half of the CISOs interviewed believe that the need to better adapt to customer needs, as well as the requirement to bring data closer to the customer, are key drivers for the increase in the role data plays in modern business.

John Meakin, former CISO at GlaxoSmithKline, BP, Standard Chartered, and Deutsche Bank, notes:
"All businesses are adapting the way they interact with their customers and staff to make more use of the opportunities for better business offered by the expanding uses of personal digital technology. This trend has of course been accelerated by the pandemic, with a rapid loss in direct, in-person interaction with customers."

It is also widely acknowledged that when properly used, data can be the disruptor that enables new offerings, growth, and customer retention. **Endré Jarraux Walls, CISO at Customers Bank**, affirms this idea, "Properly curated data helps create those 'wow' moments that keep customers loyal."

However, with the growth in the value of data, comes new challenges. One of the most obvious is unchecked growth, as **Ian Thornton-Trump, CISO at Cyjax** notes: "For too long we've been copying one server's shares to another server's shares, and we have amassed a gigantic amount of data which is of little value to the organization, but may, in fact, be considered sensitive data from the perspective of compliance."

The compliance angle is mentioned as a concern in several additional instances. **Joel Fulton, Former CISO at Symantec and Splunk**, believes that "The unexpected value, discovered from amalgamation and analysis, means it is not often predictable which data sets are valuable and which are not. This uncertainty and the potential for 'wildcat strikes' mean all data must be considered valuable until exhaustively ruled out."

Another concern voiced by most CISOs surrounds the growing need to ensure data safety and integrity – as **John Meakin** notes, "Of course, the bond we need to make with each and every customer in keeping their data accurate and secure grows all the time."

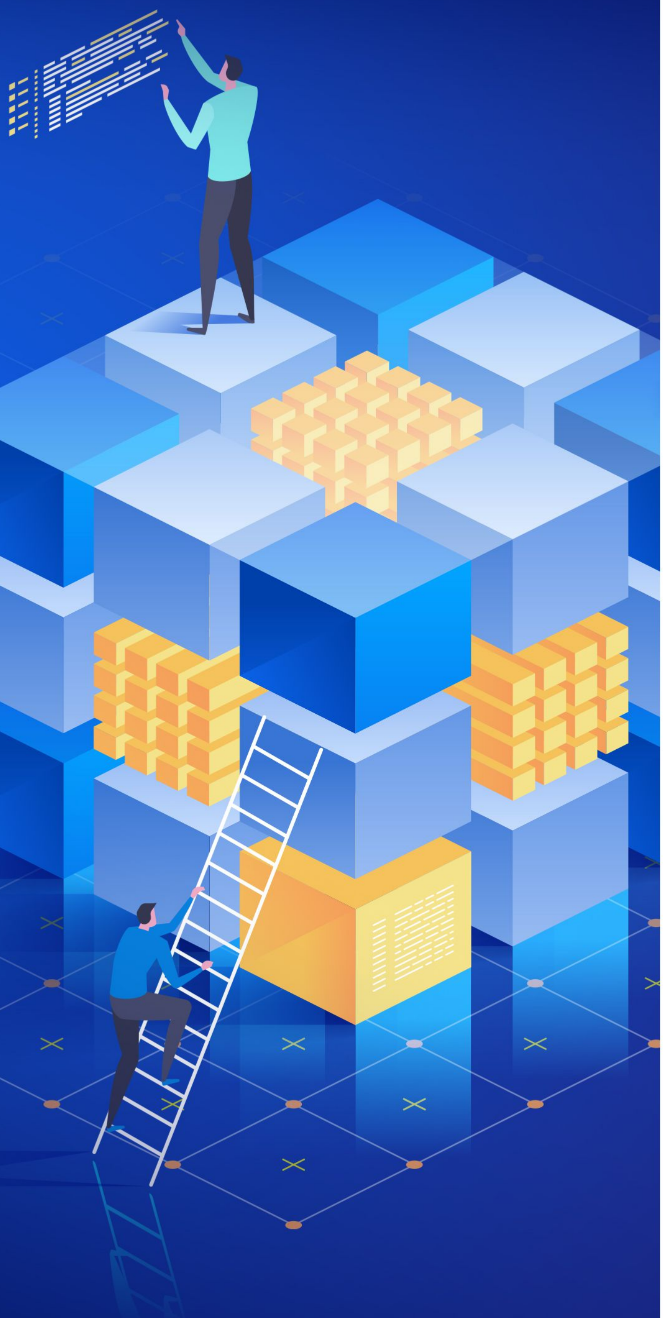
Sunil Varkey adds, "Regulations and standards are more stringent, and attacks on data integrity is a new emerging concern and consideration for many organizations."

Finally, as the value of data is realized organization-wise, more and more stakeholders launch independent and often unsynchronized data analysis initiatives – making control of who has access to the data, and what level of access is granted extremely challenging.

As **Joel Fulton** explains, "Security practitioners don't know how to control the sudden amalgamation of highly confidential data, its sudden use by disparate parties, and the desire to both share and experiment on such data."

HOW TECHNOLOGY ADAPTS

CISOs appear to have mixed feelings about how well technologies have adapted to meet the increase in data's business value. Some feel that advances in data management solutions will stay ahead of data growth, primarily through the evolution of the cloud.



However, many voice concern about technology maturity and scalability to solve real data-security challenges:

DLP (Data Loss Prevention) is widely considered as immature, or even an unfulfilled promise - **Ian Thornton-Trump** states that "Many quickly abandon the idea as "not commercially viable."

Lack of visibility - **Dick Wilkinson, Former CISO at New Mexico Supreme Court**, shares, "I would say visibility of all my data and just how easy it is for data to find a way out of your perimeter through basic human error, are two things I have always found challenging." This is expanded upon by Sunil Varkey, "The overall IT landscape is going through massive dynamic and disruptive changes. All these changes lead to a lack of visibility and more security blind spots."

Data is being targeted more and more - "Highly motivated attackers are capitalizing on the situation, with ransomware and other critical incidents becoming a routine activity," states **Sunil Varkey**.

Ashish Thapar adds his thoughts, "Organizations are increasingly dependent on third parties or service providers to leverage their digital transformation journey to enhance their business/market share. However, third party security risks often do not get as much attention as they should. Recent supply chain attacks and software repository compromises puts a spotlight on this important but overlooked piece of the security puzzle."

RANSOMWARE

RANSOMWARE

RANSOMWARE

Finally, most CISOs are extremely concerned about the rise of ransomware – not only of the proliferation of attacks, but also of their sophistication: “The storage & backup environments are now under attack, as the attackers realize that this is the single biggest determining factor to show if the company will pay the ransomware,” says George Eapen, **Group CIO (and former CISO) at Petrofac.**

Most CISOs feel that far too many attacks succeed.

Given the growing value of data, this raises significant questions about the overall maturity of storage and backup security.

SECURITY

EVOLUTION OF SECURITY PRACTICES FOR DATA, STORAGE, AND BACKUP

CISOs acknowledge that security practices need a serious refresh, with a large number of them concerned that not enough is done. “While we’re still lagging as an industry, it is good to see more and more CISOs acknowledging the risks, and beginning to properly secure their storage & backup systems,” states **Joel Fulton**.

The majority of the CISOs feel that too little focus is paid to recoverability – a shortsightedness that manifests itself in many forms:

“Threat models need to be focused on data and system ‘availability’ risks, and a huge piece of that data protection mandate is in the hands of DR/BCP capabilities.”

- Ian Thornton-Trump

When it comes to securing data assets, almost all CISOs felt that current IT management practices leave much to be desired:

“IT teams need to learn how to properly segment and maintain data to protect both the company and those who have entrusted their information to it.”

- Endré Jarraux Walls

“There’s a need to find the loopholes. No matter how consolidated you think the data has become, hunt – just as you do for threats – for the vulnerable data outside the ring of protection.”

- Joel Fulton

According to George Eapen, ensuring storage infrastructure is hardened has become one of the more recent - and most critical – areas of data security. He states that *"Storage & backup environments are now under attack, as the adversaries realize that this is the single biggest determining factor to show if the company will pay the ransomware."*

Eapen elaborates, *"Hive ransomware has been making waves since June 2021, breaching organizations through malware-laced phishing campaigns. One of the things they're known for is seeking out and deleting any backups to prevent them from being used by the victim to recover their data."*

John Meakin agreed, *"As important as it may be, data encryption is hardly enough to protect an organization's core data. If attackers find their way into a storage system (as data encryption alone won't prevent them from doing so), they are free to cause severe damage by deleting and compromising petabytes of data – whether they're encrypted or not. This also includes the snapshots and backup."*

Most CISOs expressed their hope for better guidance from vendors, and for industry effort to improve control over storage and backup environments. A few are encouraged by the recent attention to improving awareness and knowledge sharing of storage security best practices – pointing out NIST SP-800-160 for providing guidelines for architecting cyber resilience, and NIST SP-800-209 for providing detailed guidance on securing storage and backup systems.

In addition to NIST, it is interesting to note that in October 2021, Gartner® published a report, 'Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware'. In this report, they write that "I&O leaders must evaluate cyber storage solutions as a new defense mechanism to protect their most critical data."

CISOS' ADVICE TO THEIR PEERS

Focus on better policies, and better design

A common recommendation is to revisit the way organizations approach information storage and backup security. **Sunil Varkey** states that "Information protection should sit across the lifecycle of data. Starting with blueprinting an enterprise's data landscape and a relevant threat model based on confidentiality, integrity, and availability should be applied to ensure required controls are enforced through its lifecycle."

NIST SP 800-160 and 800-209 are both great resources. **Ashish Thapar** adds, "*Having solid knowledge of business processes, data flows, and systems is important – before any data protection initiatives are driven.*" **Thapar** advocates a *'Secure-by-Design'* and business-centric 'Enterprise Security Architecture' based approach for data management – which is no different from managing compute and network elements.

Joel Fulton warns against the risks of taking data management and governance too lightly. He states that, *"The key challenge protecting data as a security leader is the fact there rarely exists a data management or governance strategy. With hindsight, a security leader would strongly encourage master data management strategies and projects, unifying disparate data and applying consistent and valid controls."*

Invest in cross-team collaboration and know-how

To drive more secure storage designs, a better level of threat modeling is required. This suggests that infosec teams must go back to basics, learning more about storing and protecting data, as well backup attack surfaces. **Sunil Varkey** explains that "Asset management in my enterprise experience has been sub-optimal, so I tend to try and understand the external attack surface."

Ian Thornton-Trump advocates the importance of mentoring teams across the organization, and encouraging bridging the knowledge gap, "I think the most important one is to ensure everyone understands the meaning and intent of your security program. Be approachable and available to your organization, and align your security program to your business objectives. Finally, my advice is to use the most powerful tool for security you have: cross-team communication."

Others also comment on the need to build a high-performing team with effective tooling. For example, Dick **Wilkinson** states, "Don't underestimate the human resources it may require to effectively secure large data sets and the cost associated with data management. Don't risk underspending on security."

Wilkinson continues, "Data storage tends to be a blind spot for security teams, who up until recently 'outsourced' storage security to the IT infrastructure team – assuming they know best how to keep it secure. Analyzing data storage – at an infrastructure layer - and data protection security posture is a new skill that security teams have recently been adopting, in order to deal with emerging cyber security threats."

COLLABORATION

Implementation

The next logical step after revisiting storage and backup security architecture, and modeling threats, is to enforce strict data access controls and implement clear segmentation between environments. Sunil Varkey echoes this, “Enforcement of least privileges, control enforcement, restrict information flow channels, and generate logs for traceability [of data access, security configuration changes, and flows].”

Ian Thornton-Trump mentions that storage and backup systems are miles behind other IT layers and recommends, “In my opinion, the two pieces where CISOs should be concentrating, is moving an IDAM + MFA + SSO agenda forward.”

Recovery planning and validation

It was agreed that organizations should pay much more attention to ensuring the recoverability of data, as the paradigm shifts to the working assumption that it’s a matter of “when” not an “if” attacks will succeed – as John Meakin explains, “CISOs cannot control all the platforms, which makes data protection the only solution.” Sunil Varkey adds, “The crown jewels of any kingdom are to protect its data, and it’s not an easy task considering the many environmental changes and motivated adversaries around.”

Ian Thornton-Trump expands upon these statements, “When cyber-attacks happen, you want to ensure that the core business functions are protected. That means a solid backup strategy and the capacity to bring those systems back online if degraded or rendered inoperable.”

On-going evaluation and measurement

Sunil Varkey suggests that “Periodic risk assessments are essential to defining information protection strategies, based on criticality, exposure, vulnerabilities, controls, and threats.” He then expands, “Focus on making risk assessment continuous – and understand what ‘zero trust’ really means [in the context of securing storage and backup].”

Ian Thornton-Trump echoes these statements, “Secure backups and snapshots are required of all business systems, and the CISO that wants a daily report on that status is a wise CISO!”

John Meakin summarizes, “And monitor, monitor, monitor…”

Ashish Thapar offers this advice, “Engage early in the cycle – adopt a ‘Shift Left’ approach for all new [storage and backup] initiatives.” And he stresses the need to get a seat at the table: “Ensure you involve board members on being aware of the risks and corresponding mitigations to ultimately drive Cybersecurity Investment Prioritization.”

Finally, Joel Fulton concludes, “Find the loopholes. No matter how consolidated you think the data have become, hunt – just as you do for threats – for the vulnerable data outside the ring of protection.”

CLOSING WORDS

We are grateful for the valuable insights generously shared by all participating CISOs, who represent a wide range of industries and disciplines.

It is evident that the value of data is well recognized, and that the concern of data-targeted attacks is real and present across all ranks of organization leadership.

Since there's no realistic way to completely bulletproof an organization, it is becoming evident that the storage and backup services are truly the last line of defense.

The participating CISOs were united in several key concerns:

01

Technology is not evolving fast enough. While many capabilities adapt, the pace is not quick enough, and securing the storage infrastructure is still a hit and miss thing. There's definite innovation (e.g., immutable storage, offsite cloud archives, threat intelligence) – but it mostly involves discrete capabilities that do not blend in well.

02

Visibility and control: infosec practitioners do not have sufficient visibility and control over the security posture of the storage and backup planes. Infrastructure and infosec teams do not share the same security vision – and at times even have conflicting interests.

03

Process: there's much room for improvement across multiple stages of the data management lifecycle: from better classification to clear and detailed definition of security baselines – through visibility and governance

CISOs are also unanimous in recommending a much tighter control loop. A 'shift-left' approach should be widely adopted, implying that storage and backup security should be continually evaluated, tested, and improved.

Tighter regulation and government involvement is perceived as both a burden (at least in the short term) and a blessing. The increased focus on data security means better guidance, and better national – or even international coordination.

DORON PINHAS

CTO, Continuity and Co-Author of the NIST Special Publication 800-209 'Security Guidelines for Storage Infrastructure'

CONTINUITY

WWW.CONTINUITYSOFTWARE.COM