IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The Pervasiveness of Data and Data-Centric Security Strategy

Adam Strange

Adam Strange
Global Marketing Manager
Titus, by HelpSystems

Biography

Adam Strange heads up the global marketing function at Boldon James, and is the Global Marketing Manager for Titus, by HelpSystems (https://www.titus.com), working to define and implement our strategic go-to-market campaigns. He brings a proven and successful record of managing integrated business-to-business marketing activity to both increase brand profile and capture leads and opportunities.

Adam has a widespread understanding of enterprise IT infrastructure across areas such as Cybersecurity, Threat Intelligence, Cloud-based Services, Business Applications, Databases and Hardware.

Prior to Boldon James, Adam ran the marketing and alliances function at Becrypt, and has held former marketing and partnering positions at BAE Systems, Oracle and Computacenter.

Keywords Data security, Data privacy, Data loss prevention, Digital Rights Management (DRM), Human error, Information security, CISOs
Paper type Research

Abstract

In this last year, we have seen an exponential growth in not just the amount of digital data, but also its vulnerability. Data breaches are becoming daily news, and security and risk management spending is set to reach $150 billion this year, as businesses struggle to build a strong perimeter to ensure information security. But what if 'building walls' is the wrong approach? In this article, the author illustrates the pitfalls of information security architecture and explains how shifting to data-centric strategies will protect data at file-level throughout its entire life cycle.

Introduction

Regardless of what business you are in, a data security breach is an increasingly likely scenario that all businesses must mitigate. With escalating cybercrime, the widespread growth in Cloud computing[1], and the explosion in mobile devices and varying tech and app use amongst employees and partners; key aspects of enterprise security are now, and will forever be, beyond our control.

In fact, Gartner has forecasted[2] that security and risk management spending worldwide will grow 12.4% to reach $150.4 billion in 2021. Even with that investment, the number of data breaches is increasing.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The pervasiveness of data and the complexity of the underlying environment continues to increase by orders of magnitude, and increased vulnerability around sensitive data is here to stay for all businesses. But for CISOs, is it merely a question of continually bolstering an organization's core defenses – the systems, applications, devices and networks that enclose data?

The fact is that with more apps, more data, more networks, and more logins than ever before, sensitive data may be at risk out of sight and beyond the reach of security teams. Gaps in security policy and process will always exist and a policy of 'building walls' with strong perimeter-based security, authentication, encryption and more will sometimes fail.

The four key gaps in information security architecture

There are four key gaps[3] in information security architecture that revolve around employee and external partner behaviours, and can only be remedied with data-centric security practice (and by engendering a solid security culture within the business). For CISOs these pain points pose serious risks in terms of maintaining compliance and can create a reactionary environment of playing continual catch-up.

1. **The Behavior Gap:** Usability poses a major challenge to CISOs. People simply want to find the fastest, most convenient way of doing something. In fact, human error is still the number one cause of data breaches in 2021[4]. Sensitive files will be added to USBs or data copied to unsecured documents, secure FTP servers may be bypassed, and people may not always adopt the security processes in place.

2. **The Visibility Gap:** Sensitive data travels. Average employees send emails in their tens of thousands per year and many receive files they were not meant to see. IT Governance lists a staggering number of serious enterprise data breaches[5] in March 2021 alone.

   Who accesses data once it's shared beyond a business's devices, networks, and applications and how it is used is beyond your control and lies outside of your monitoring, auditing, and tracking technologies.

   Where files and data are shared outside your organization, the nature of the information within them cannot be tracked or audited once it leaves your server.

3. **The Control Gap:** Lost files or leaked information can go beyond an organizations control. Identity and Access Management[6], Mobile Device Management and Data Loss Prevention (DLP) systems[7], all help to monitor and control employee access to data. But data that leaves the systems and networks within your sphere of influence is effectively out of your control.

   Lost or leaked information can bear serious consequences with no way to shut down the information once leaked, and potential violations that must be reported with implications around compliance.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

4. **The Response Time Gap:** There is a time lag between uptake of a new application or behavior and the ability of CISOs to understand and respond. It's what puts security teams into reactionary mode and can take weeks or months to identify, during which time you don't know what's happening with sensitive information.

Technology changes quickly and in many organizations employees bring their own devices, applications, and expectations of how to work. Departments purchase applications and devices, which in turn generate more sensitive, proprietary information.

In the rush to get business done, security is often left to play catch-up and security breaches may be the unintended consequences of this gap.

Security needs to operate at the speed of business, with flexibility to adapt to the unknown. Your Response Time Gap may be measured in days, weeks, months, or quarters. The longer it is, the greater the risk of people taking measures into their own hands, or of sensitive data going untracked into new applications.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Closing the data security gap with data centric security strategies

Collaboration, innovation, partnerships, and business development are the behaviors that drive business growth and all are dependent on trusted exchanges of vital information.

When these new unforeseen breaches take place, CISOs must respond by evolving from infrastructure-centric security measures with multiple layers of defense, to data-centric approaches[8] that protect what really matters: the data itself.

Data Loss Prevention (DLP) solutions, data encryption solutions and Digital Rights Management (DRM) tools often take a limited view of the data to be protected, for example files on a server or emails leaving the network, and they still depend on the idea of walls – systems, devices or networks that enclose data.

Businesses need to be able to guarantee file-level security – to secure, track and share any kind of data, no matter where it's stored or located, with robust policy enforcement, strong encryption, and strict access controls. Data-centric security solutions also enable employees to collaborate freely while ensuring a high level of security and visibility, and even revoke access to sensitive data that has been shared by email mistakenly. Furthermore, by adding a cloud-based tether, access to data can be managed with access rights and the data decrypted if the person is approved.

Data is the lifeblood of business and, by locking it down too tightly, business slows down and potentially diminishes its value. CISOs should adopt a data-centric security solution that secures sensitive data through its entire life cycle; everywhere it travels, no matter who has it or where it's stored. By adding in this additional layer of security, data is protected in motion, in use, or at rest, inside or outside the organization.

Reference

1 'The Global Cloud Computing Market is expected to grow by $ 287.03 bn during 2021-2025, decelerating at a CAGR of over 17% during the forecast period' (23 April 2021), Intrado GlobeNewswire. Available at: https://www.globenewswire.com/news-release/2021/04/23/2216012/0/en/The-Global-Cloud-Computing-Market-is-expected-to-grow-by-287-03-bn-during-2021-2025-decelerating-at-a-CAGR-of-over-17-during-the-forecast-period.html

2 Hurst, A. (17 May 2021) 'Worldwide security and risk management spending to exceed $150 billion in 2021 — Gartner', Information Age. Available at: https://www.information-age.com/security-risk-management-spending-exceed-150-billion-2021-gartner-123495197/

3 Vera, (2016) 'The Definitive Guide to Data Security - Taller walls aren't the answer' (2016), Vera by HelpSystems, Available at: https://www.vera.com/wp-content/uploads/2016/06/Vera-Definitive-Guide-To-Data-Security.v2.pdf

4 Maslow, J. (4 March 2021), 'Human error is still the number one cause of most data breaches in 2021'. Influencive. Available at: https://www.influencive.com/human-error-is-still-the-number-one-cause-of-most-data-breaches-in-2021/

5 Irwin, L. (1 April 2021), 'List of data breaches and cyber attacks in March 2021 – 21 million records breached', IT Governance. Available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-march-2021

6 HelpSystems, 'Identify and Access Management: Secure your system by managing user privileges and access to sensitive data – without getting in the way of productivity', HelpSystems. Available at: https://www.helpsystems.com/solutions/cybersecurity/identity-access-management?

7 Clearswift, 'Data Loss Prevention - Adaptive DLP for Real-time Data Loss and Content Threat Protection', Clearswift by HelpSystems. Available at: https://www.clearswift.com/solutions/adaptive-data-loss-prevention?

8 Vera: Titus policy engine brokers VERA encryption, Titus by HelpSystems. Available at: https://www.titus.com/tech-partners/vera?