avancer
Simplified IT Security

SEVEN MUST-FOLLOW TIPS TO REDUCE SECURITY BREACH COST

The current pandemic situation escalated ransomware and phishing scams, with cybercriminals taking advantage of insecure systems and networks, impacting both large and small businesses.

Tel : (609) 632-1285 | Email : info@avancercorp.com
101, Interchange Plaza, Suite 201, Cranbury NJ 08512, USA

Shift to remote working due to COVID-19 anticipated to further increase the cost of a data breach, with the average total cost of a data breach of USD 3.86 million jumping up to USD 4 million, as per another report by IBM. The remote workforce will also pose security challenges, which will increase the time taken to identify and contain a potential data breach.

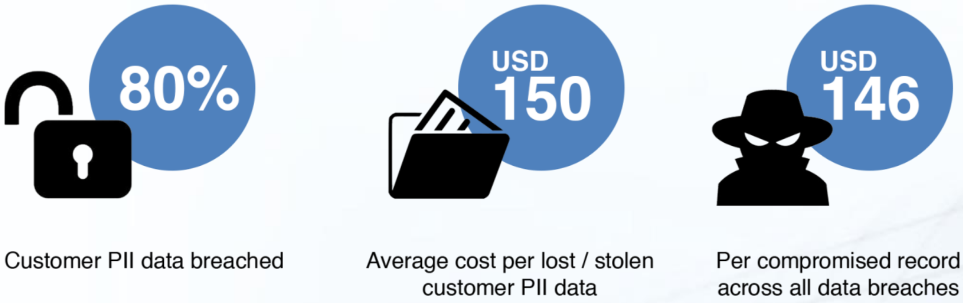
However, the most worrying aspect of data breaches remains the compromise of customers' personally identifiable information (PII). As per the IBM report, in comparison to other types of data, 80 percent of the breached data were that of customer PII. Further, while the average cost per lost or stolen record for customer PII stood at USD 150 per record, it was at USD 146 per compromised record across all data breaches[i].

Average cost of a data breach during pandemic:

USD 21,659 per incident
Cost of data breach incidents range: USD 826 to
USD 653,587

5 per cent of such successful attacks cost the businesses USD 1 million or more

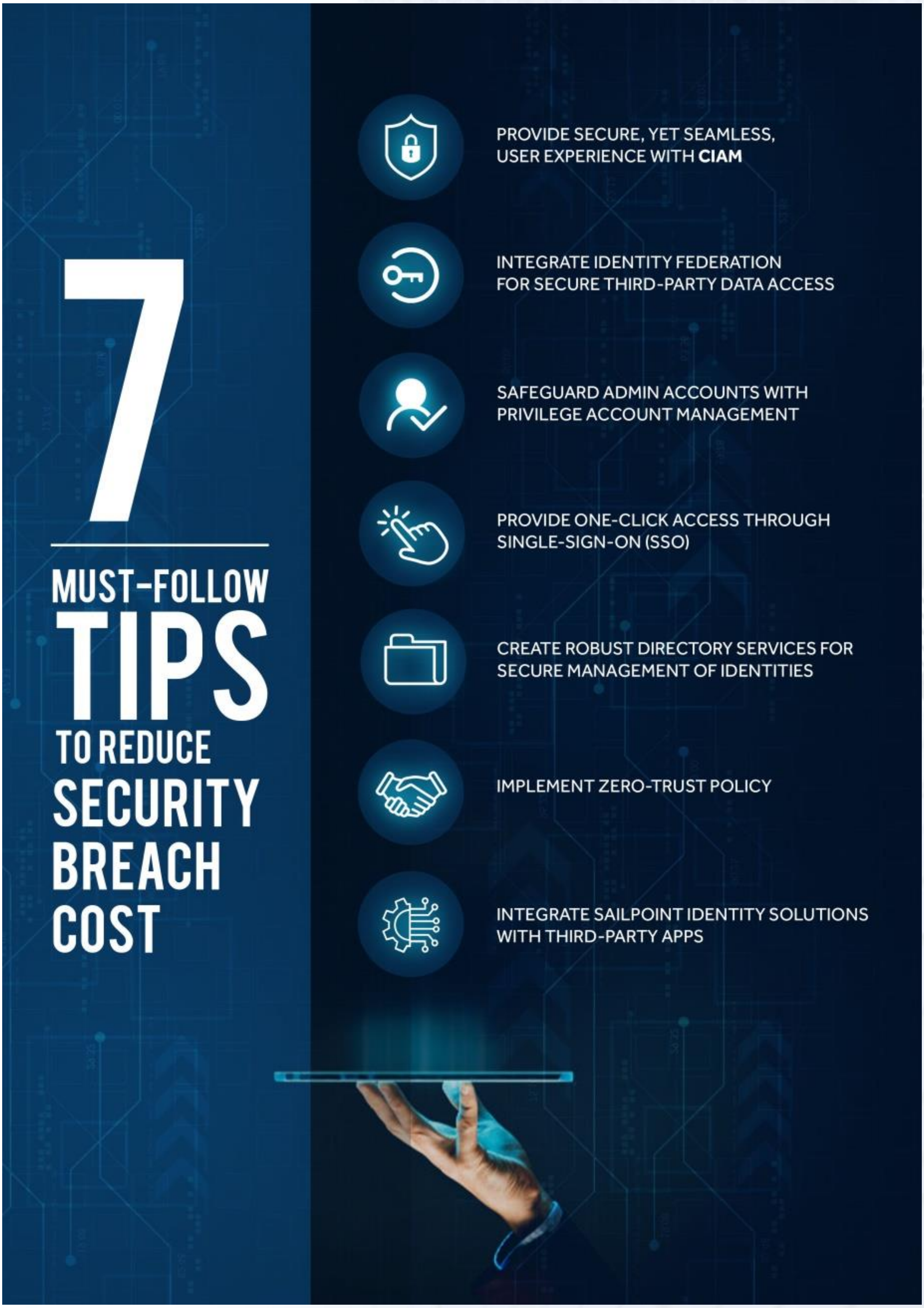
Source: Verizon: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf



Source: IBM: https://www.ibm.com/downloads/cas/RZAX14GX

The trend is expected to continue with global cybercrime costs predicted to increase at the rate of 15 percent annually for the next five years, reaching a massive USD 10.5 trillion by 2025[ii]. Along with denting the revenue of the company, data breaches also result in intangible damages such as causing distrust amongst customers and a negative brand reputation.

We explore in this article, seven must-follow effective methods to prevent data breaches and thereby, reducing security breach costs. As a breach of user data or identity data is the most crucial data breach for any organization, we focus on how to reduce breaches and prevent unauthorized access to such data with the implementation of various identity and access management (IAM) solutions.



7 MUST-FOLLOW TIPS TO REDUCE SECURITY BREACH COST

- PROVIDE SECURE, YET SEAMLESS, USER EXPERIENCE WITH **CIAM**
- INTEGRATE IDENTITY FEDERATION FOR SECURE THIRD-PARTY DATA ACCESS
- SAFEGUARD ADMIN ACCOUNTS WITH PRIVILEGE ACCOUNT MANAGEMENT
- PROVIDE ONE-CLICK ACCESS THROUGH SINGLE-SIGN-ON (SSO)
- CREATE ROBUST DIRECTORY SERVICES FOR SECURE MANAGEMENT OF IDENTITIES
- IMPLEMENT ZERO-TRUST POLICY
- INTEGRATE SAILPOINT IDENTITY SOLUTIONS WITH THIRD-PARTY APPS

#Tip 1: Provide a secure, yet seamless, user experience with CIAM. Businesses are now focusing on providing a digital-first experience to their consumers at every juncture, resulting in the creation of more new accounts and accessing existing accounts regularly. Thus, enterprises must deal with more identity credentials, while safeguarding them from cyber attackers who are undertaking sophisticated and targeted attacks. Consumer/Customer Identity and Access Management (CIAM) brings a technological solution that provides a mechanism to store customer profile data, authentication services, along with helping to manage identities and securing data across all channels. It integrates a strong security layer in the entire user journey right from the process of logging to minimize the threat paradigm and achieve compliance with important regulations such as General Data Protection Regulation.

#Tip 2: Integrate identity federation for secure third-party data access. Federated access management enables enterprises to enforce identity and role-based access control policies for users outside an organization's borders. It allows setting up policies to distribute just the right information among users, reducing the threat of data security breaches. Such a solution minimizes manual informational sharing and external user-related data sharing risk by enabling users of the external domain to access data or systems resting securely and seamlessly in the enterprise domain.

#Tip 3: Safeguard admin accounts with Privileged Account Management. Attacks caused through system administrators' accounts can cause substantial loss to an organization. As admin accounts have greater controls over IT systems, any malicious entrant can cause significant damage to systems, by breaching the IT systems through the credentials of a superuser. Implementation of a Privileged Account Management solution allows businesses to enforce credible access authentication and authorization of privileged users. In addition, it brings ease in the management of password and access disclosure to satisfy basic policy and regulatory requirements.

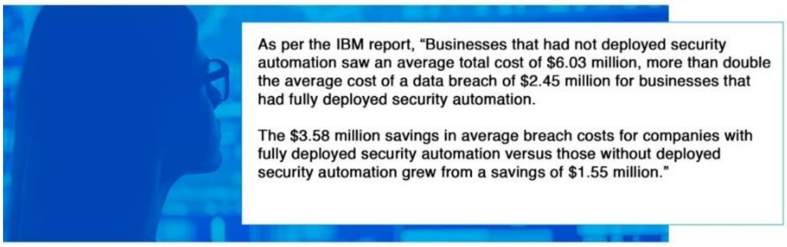
#Tip 4: Provide one-click access through Single-Sign-On (SSO). With the help of SSO, users can authenticate their identity and access multiple applications with a single login, thus eliminating the reuse of a password and minimizing the chances of phishing attacks. SSO enables customers, employers, and partners to get seamless access to a wide range of applications and devices – including mobile, SaaS, cloud, and enterprise applications – without the hassle and the security challenges of duplicate accounts, VPNs, passwords, and multiple logins. Such as centralized identification system eases off the burden for an enterprise by lowering instances of login troubleshooting, as well as data breach attacks.

#Tip 5: Create robust directory services for secure management of identities. Active Directory Management helps in bringing together resources, users, networks, and access points, enabling better management of users with departmental access to corporate services and business resources. Thus, creating a robust directory that authenticates users for any enterprise-level application paves way for tightening security, increased productivity, and improved business continuity.

#Tip 6: Implement Zero-Trust Policy. Zero Trust policy focuses on an organization's ability to monitor and secure user's identities and access points in a consistent manner. It ensures that any user logging on to the system is being identified constantly and their access is managed consistently, no matter their designation or role in the organization, thus, minimizing any chances of breaches.

#Tip 7: Integrate SailPoint identity solutions with third-party apps. Get complete identity solutions with SailPoint products, such as SailPoint IdentityNow and SailPoint IdentityIQ. Enterprises can also integrate them with third-party applications, such as Epic, Cerner, Office 365, ServiceNow and SAP, to reap the benefits of managed services, role-based access control, password management, identity management over the cloud, and others.

Source: https://www.ibm.com/downloads/cas/RZAX14GX



As per the IBM report, "Businesses that had not deployed security automation saw an average total cost of $6.03 million, more than double the average cost of a data breach of $2.45 million for businesses that had fully deployed security automation.

The $3.58 million savings in average breach costs for companies with fully deployed security automation versus those without deployed security automation grew from a savings of $1.55 million."

Implementing the above solutions would ensure not only securing the enterprise IT ecosystem but also augmenting the revenue for the company on the back of a robust corporate system and network. Undertaking security measures have proved to be beneficial for reducing the cost of data breaches. With an increase in cyberattacks, specifically focusing on malicious breaches, stolen credentials, insider threats, ransomware, and malware attacks, it has become imperative to undertake the above recommendations to safeguard enterprise data, along with potential financial and reputation damage.

How Avancer can help?

Data breaches can have extensive impact on the finances, reputation, and credibility of an enterprise, effecting an organization's operations and compliance in the short-term, while leading to loss of business and competitive disadvantage in the long-term. To safeguard businesses from potential data breaches, our experts are at the forefront in identifying and addressing vulnerabilities in enterprise systems, networks, and applications through our robust security measures.

We have more than two decades of experience in identity governance and managing the threat landscape. With the implementation of our customized identity management solution, we have been able to help organizations to secure their user access, become compliant with regulatory policies, mitigate risks and minimize costs associated with data breaches.

[i] https://www.ibm.com/downloads/cas/RZAX14GX
[ii] https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Corporate Headquarters

101 Interchange Plaza,
suite 201
Cranbury, NJ 08512

Tel: 609 632 1285
Fax: (877) 843-8594
Email: info@avancercorp.com
https://www.avancercorp.com

About Avancer

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, it has over a decade's expertise in the field of Identity and Access Governance and IT Security. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products, and services focused on IAM Technology. Our services range from full-term project life-cycle implementation to tailor-made short-haul projects including software procurement, architectural advisement, design, and development through deployment, administration, and training. For More Information, please visit https://www.avancercorp.com