## OVERVIEW

### "S" in Default is for Security

Security Misconfigurations occur when trusted users such as IT, DevOps teams, or even contractors deploy servers or software in ways which can be easily abused. For example, provisioning a database in the cloud with no password enabled, or even with a well known default like "admin/password." Even organizations that are not deploying traditional databases, and instead using technologies like Amazon Web Services S3 Buckets can be vulnerable. Palo Alto Networks 2020 Cloud Threat Report found that 13% of templates were configured to allow internet-wide access to S3 buckets, and services such as GrayhatWarfare's Bucket Search allow quick searching to see what data is available.

IBM XForce's Threat Intelligence Index 2020 painted a staggering picture of the cost of security misconfigurations, which they categorized as "publicly accessible cloud storage, unsecured cloud databases, and improperly secured rsync backups, or open internet connected network area storage devices." The report found that 8.5 billion records were compromised due to these misconfigurations, over 200% greater than in 2019, and accounted for 86% of the total records compromised in 2019. However, the total number (frequency) of misconfiguration incidents declined, which means that the overall severity of the incidents skyrocketed.

One significant incident of this nature happened in the fall of 2019 when a customer of PeopleDataLabs unwittingly left an unsecured datastore open to the internet, exposing 1.2 Billion records of aggregated data on social media profiles. Because the customer is unclear, the legal and financial impact is still unclear. In a more recent example, a class action lawsuit was recently filed against the University of Washington Medicines data breach for the exposure of nearly 100 million records, which patients were finding online with simple Google searches. The data was exposed online for approximately 1 month, which highlights the importance of controls against these misconfigurations.

## BEST PRACTICE

### Security Misconfiguration Resulting in Data Breach

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's model for a data breach caused by a security misconfiguration recommend that organizations do the following to prevent and mitigate these attacks:

- Ensure the Devops teams use tools to detect misconfigurations in infrastructure templates

- Use Attack Surface Monitoring software to periodically (and ideally, continuously) monitor your organization's internet footprint to detect common vulnerabilities on your internet-facing infrastructure
- Avoid deploying default configurations for applications, especially with respect to passwords and authentication.
- Use a password manager to share necessary group logins and configurations.

## INSURANCE

### Breach of Privacy

Cyber insurance policies should cover more than just hacks. Misconfigured systems can expose legally protected data and threaten the operations of your business. Policies should also cover the steps you'll need take to make sure no data was stolen - and how to respond if it was. Speak with your broker to learn more.

### Example Claim

A state government misconfigured the servers on which it saved its employee records, including financial, retirement, and pension data, leading to the records' exposure on the internet. Policies should cover legal and forensic investigation necessary to determine whether anyone had unauthorized access to the data, what data breach laws were triggered, and how to fulfill those legal obligations. When state data breach notification statutes are triggered, policies should cover the costs of notification, call center, and provision of credit monitoring.