



beyond cybersecurity

Volume 3 | Issue 4 | April 2019

# GDPR



## A YEAR ON



# PROVISE FOR YOU

- ProVise is an Independent, product agnostic research driven Advisory firm specializing in GRC and Cyber Security Professional Services.
- What started with two people in 2011 is now an entity spanning across regions with a global portfolio of leading customers.
- Since its inception in 2011, ProVise has expanded its footprint in 7 countries and has around 175+ Successful projects executed.
- As of today, ProVise is a Trusted cyber security partner in UAE for the Largest Police Force, Largest Real Estate Firm, Largest Telecom Company, Largest Entertainment Island and striving for much more.

## OUR BUSINESS LINES



Technology Governance, Risk and Compliance advisory business

- WINNING IS NOW A HABIT IN PROVISE



Industry specific , Threat Centric Cyber Security Assurance and Monitoring

- R&D IS THE CORE OF ALL SERVICES AND PROJECTS



Product Engineering and R&D is located in Bengaluru.

- GRC COGNITIVE PLATFORM • CYBER SECURITY PLATFORM

## OUR DNA

Dream is not that which you see while sleeping, it is something that does not let you sleep.

**Vision**  
To be the customers partner of choice for safeguarding their digital assets



innovation distinguishes between a leader and a follower

## Mission 2021

- Top 3 Cyber Security Research Firms in Asia
- No.1 GRC Platform Globally
- No.1 GRC Consulting Firm Globally



**08**  
**BUZZ**  
Top 10 Neglected Data Security Best Practices



**08**

**16**  
**UNDER THE SPOTLIGHT**  
Ben Aung  
Global Chief Information Security Officer, Sage



**16**

**26**  
**INSIGHT**  
Crucial Cybersecurity Assessment Steps Before Merger or Acquisition



**26**

**36**  
**COVER STORY**  
GDPR a year on, busting the myths and exploring the new realities



**36**

**46**  
**COLLABORATIONS**  
InfoSec Partnerships



**46**

**54**  
**IN THE NEWS**  
Top Stories from the Cybersecurity World



**54**

**62**  
**IN THE HOTSEAT**  
High-Profile Appointments in the Cybersecurity World



**62**

**68**  
**KICKSTARTERS**  
Startups Making Waves in the Cybersecurity World



**68**



## EDITOR'S NOTE

The General Data Protection Regulation (GDPR) came into force in the European Union on May 25, 2018. It's been a year now, and a lot has changed around data protection legislation across the European Economic Area (EEA). GDPR became an opportunity for several companies to establish best practices in cybersecurity, and it also paved way for California Consumer Privacy Act that is touted to be the GDPR for the United States of America. The U.S. is one of several nations in the world to join the bandwagon of data protection. In other words, the juggernaut has rolled.

In our Cover Story, we bust several myths around GDPR that still persist while also exploring newer realities. In our Buzz section, we explore several neglected data security best practices including classification of data based on its sensitivity, password management for admins, reviewing data available to everyone, among several others.

We have Ben Aung, Global Chief Information Security Officer of Sage, Under the Spotlight as he talks about how GDPR affected businesses, and discusses the gray areas in GDPR that companies are still struggling to understand. In our Insight section, we shed light on methods to protect yourself before a merger or an acquisition by detailing several cybersecurity assessment steps your organization can follow.

Tell us what you think of this issue. If you have any suggestions, comments, or queries, please reach us at [editorial@cisomag.com](mailto:editorial@cisomag.com).

**Jay Bavisi**  
Editor-in-Chief

# CISO MAG

beyond cybersecurity

Volume 3 | Issue 4  
April 2019

Editorial  
International Editor  
**Amber Pedroncelli**  
[amber.pedroncelli@eccouncil.org](mailto:amber.pedroncelli@eccouncil.org)

Principal Editor  
**Rahul Arora**  
[rahul.arora@eccouncil.org](mailto:rahul.arora@eccouncil.org)

Senior Feature Writer  
**Augustin Kurian**  
[augustin.k@eccouncil.org](mailto:augustin.k@eccouncil.org)

Feature Writer  
**Rudra Srinivas**  
[rudra.s@eccouncil.org](mailto:rudra.s@eccouncil.org)

Media and Design  
Media Director  
**Saba Mohammad**  
[saba.mohammad@eccouncil.org](mailto:saba.mohammad@eccouncil.org)

Sr. Graphics Designer  
**Sameer Surve**  
[sameer.s@eccouncil.org](mailto:sameer.s@eccouncil.org)

Management  
Executive Director  
**Apoorba Kumar\***  
[apoorba@eccouncil.org](mailto:apoorba@eccouncil.org)

Senior Director,  
Compliance & Governance  
**Cherylann Vanderhide**  
[cherylann@eccouncil.org](mailto:cherylann@eccouncil.org)

Deputy Business Head  
**Jyoti Punjabi**  
[jyoti.punjabi@eccouncil.org](mailto:jyoti.punjabi@eccouncil.org)

Marketing and Business Development  
Officer  
**Riddhi Chandra**  
[riddhi.c@eccouncil.org](mailto:riddhi.c@eccouncil.org)

Digital Marketing Manager  
**Jiten Waghela**  
[jiten.w@eccouncil.org](mailto:jiten.w@eccouncil.org)

Publishing Sales Manager  
**Taruna Bose**  
[taruna.b@eccouncil.org](mailto:taruna.b@eccouncil.org)

Technology  
Director of Technology  
**Raj Kumar Vishwakarma**  
[rajkumar@eccouncil.org](mailto:rajkumar@eccouncil.org)

\* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora. The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.



Download our Cloud Security Toolkit to help you evaluate potential cloud vendors.



<http://bit.ly/2ivU4l9>

Get insight into how other companies are approaching cloud opportunities, and instill confidence across your organization today.

## From the CISO Perspective to Cloud Security Assessments

Learn How to Make the Leap With Confidence

### **The secret is out:**

Enterprises large and small have moved to the cloud, and more are making the move daily. Whether you're an early adopter or you've been battling that persistent strain of nephophobia going around, it's important to thoroughly understand and evaluate potential cloud vendors, instilling confidence for your organization and your customers.



# TOP 10

## Neglected Data Security Best Practices

Ilia Sotnikov, Vice President,  
Product Management, Netwrix



**E**nsuring data security becomes harder every day. Firstly, sensitive data is often spread across on-premises and cloud-based storage locations, which makes it more difficult to maintain security controls. Secondly, the volume of data, including sensitive information, continues to grow, which means that more data requires protection. Finally, cyber criminals get more innovative all the time. As a result, securing data in compliance with increasingly complex regulations is a challenge.

The [2018 Netwrix IT Risks Report](#) explores how organizations are working to ensure compliance and beat cyber threats. Unfortunately, the results indicate that organizations aren't doing enough to defeat the bad guys. Here are the 10 most neglected security best practices:

### 1. Classify data based on its sensitivity

Security experts recommend that organizations classify data at least twice a year, so they can reset access rights and ensure that only the right people have access to data.

**Reality check:** 64% of organizations admit that they classify data based on its level of sensitivity just once per year or even less frequently.

**Pro tip:** Many organizations rely on users to classify data, which rarely works well. Look for data discovery and classification products that automate the classification process.

### 2. Update data access rights

To prevent unauthorized access to data, security experts recommend strictly enforcing the least-privilege principle, as well as reviewing access rights every six months and after important events like an employee termination.

**Reality check:** 51% of organizations do not update data access rights even once a year.

**Pro tip:** Look for governance solutions that can assess and control access rights, both as part of an ongoing process as well as ad hoc. Also look for reporting and alerting tools that can ensure it's all being done correctly and securely.

### 3. Review data available to everyone

To reduce risk to sensitive data, security experts say that at least every three months, organizations should check that folders and shares available to everyone don't contain sensitive data.

**Reality check:** 76% of organizations are not doing this frequently enough, and some never do it at all.

**Pro tip:** Look for solutions that can automate a continuous program to discover, classify and secure





content regardless of where it resides, so you can reduce your attack surface.

#### 4. Get rid of stale data

When you no longer need data for daily operations, it should be archived or deleted. To mitigate security risks, experts recommend doing this every 90 days.

**Reality check:** Only **18%** of organizations delete unnecessary data once a quarter, meaning that **82%** of organizations are needlessly increasing their threat exposure.

**Pro tip:** Deploy an automated solution that can find stale data and collaborate with the data owners to determine which data can be archived or permanently deleted.

#### 5. Conduct asset inventory regularly

Security experts encourage you to identify all your assets (e.g. databases, software and computer equipment) and determine who is responsible for them at least once a quarter.

**Reality check:** Just **29%** of organizations stick to the recommended schedule.

**Pro tip:** Choose an asset tracking solution that streamlines data collection and analysis to locate every asset within your company. Make sure it is easy to use and fits your needs.

#### 6. Update and patch software promptly

Installing security updates to your software in a timely manner enables you to mitigate vulnerabilities. The recommended frequency depends on patch and system importance and other factors; it varies from weekly for critical security patches to quarterly for less urgent patches, such as maintenance patches.

**Reality check:** **33%** of organizations do not update their software even once in 90 days.

**Pro tip:** Establish a dedicated testing environment or at least a segment for patch testing to avoid incompatibility or performance issues.

#### 7. Perform vulnerability assessments

Regular vulnerability assessments help you locate security gaps and reduce your exposure to attacks. Security experts recommend running these assessments at least once a month.

**Reality check:** **82%** of organizations do this only twice a year or don't do it at all.

**Pro tip:** Find products that can continuously evaluate threats to your data and make sure you know which threat actors do most harm to your business. Even better, find tools that provide alerts to reduce the number of false alarms.





**SUBSCRIBE NOW**  
**FOR COMPLETE ISSUE**

### 8. Create and maintain an incident response plan

There are several parts to a well-thought security response plan: Draft a plan, get it approved, regularly train employees, and do test runs.

**Really check:** 80% of organizations admit to falling to exercise all these steps.

**Fix it:** Conduct regular tests to see how effective and realistic your team is security threats and evaluate how your plan is working in real life.

### 9. Update admin passwords regularly

If an administrator's credentials are compromised by attackers, whether the credential is shared or not, the entire IT infrastructure is at risk. Security experts recommend changing admin passwords at least every quarter.

**Really check:** Only 30% of organizations change their admin passwords at least once every 90 days.

**Fix it:** Don't use shared admin passwords, even if you update them every week. Each privileged user should have their own admin credentials and the passwords should be changed regularly.

### 10. Update user passwords regularly

While the goal of these articles is to get administrative credentials, the gateway to that information

is often times accessing a user's credentials. A security best practice is to require users to change their passwords at least every 90 days.

**Really check:** 80% of organizations mandate a password change less frequently than once a quarter.

**Fix it:** Require users to choose strong passwords (with a minimum number of characters and symbols) and change them once every 90 days. Also consider deploying multi-factor authentication and single sign-on.

Following these security best practices can help you reduce your attack surface and minimize the risk of security and compliance issues. Regularly implementing security best practices such as finding, classifying and securing your data is essential to preventing attackers from stealing your sensitive data and raising your company's reputation. **■**

The opinions expressed within the article are the personal opinions of the author. The facts, opinions and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.