THE SCALERS

A Guide to Cybersecurity for Globally Distributed Teams

Introduction

Though many businesses are embracing the concept of **building globally distributed teams**, some are still concerned about the security of offshoring.

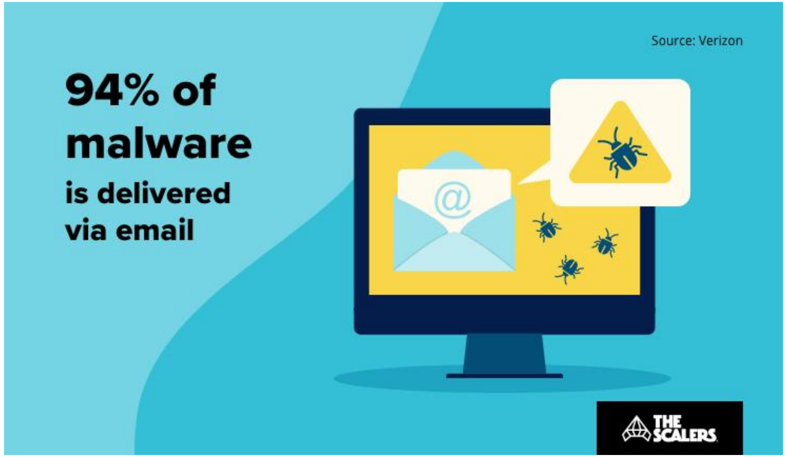
Decades of low-quality outsourcing and exaggerated horror stories have led to businesses questioning the security of their **confidential data** with their remote team.

In this piece, we'll walk you through some **data security practices** that you can implement when working with global teams to mitigate security risks and protect sensitive data.

1. Find the most secure model for your business

When you're considering **hiring a global workforce**, you can either employ freelancers, outsource your development processes, or build an offshore team.

- Hiring freelancers
- Outsourcing
- Offshoring



1. Find the most secure model for your business

Hiring freelancers:

While going the freelancer route may reduce your **operational costs**, it will also expose your business to significant security risks because you cannot monitor the people you hire.

Outsourcing:

Outsourcing agencies are **third-party vendors**, and the developers they hire are not a part of your organisation. In fact, they may even be simultaneously working for other clients.

In such a scenario, ensuring that there is no security breach is next to impossible.

Offshoring:

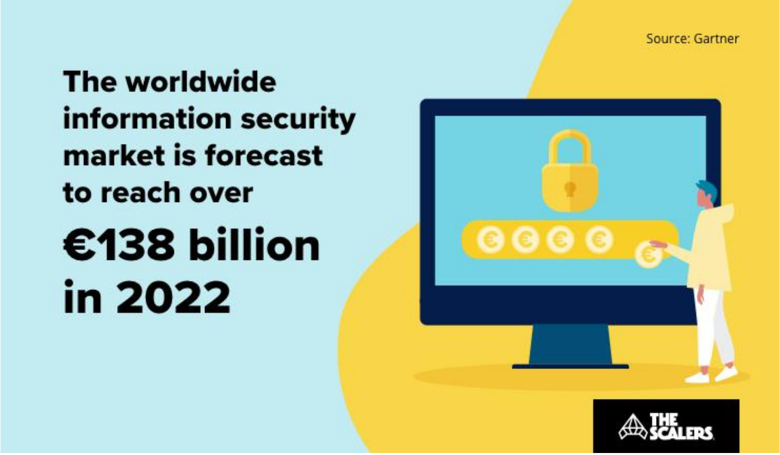
Building a **dedicated offshore team** means permanently hiring a handpicked group of individuals who are 100% part of your organisation. The only difference is that they sit elsewhere.

And because they only work for you, implementing and monitoring cybersecurity processes becomes that much easier.

2. Secure all applications and devices

Ensuring that your **IT infrastructure** is configured correctly is key when working with **distributed teams.** Some ways to do this include:

- Encrypting and installing firewalls
- Worldwide information security
- Secure access to all company systems



Source: Gartner

The worldwide information security market is forecast to reach over

€138 billion in 2022

2. Secure all applications and devices

Encrypting and installing firewalls

Installing security patches and updating the security software on all endpoints provides personal firewalls, applicational control, **antivirus protection**, and antispyware protection.

Worldwide information security

Ensure that all computer and external hard drives are encrypted to protect worker endpoints from **unwanted access**. Endpoints must also be equipped with remote wipe capabilities.

Secure access to all company systems

When working with distributed teams, restrict system access to specific networks or locations. And if any employee wants to log in from a different site, they can do so only once their **network/location is authenticated**.

3. Assess and engage safe cloud providers

Without implementing the **proper security measures**, files in the cloud can be accessed by those who do not belong to your company.

Here's what you can do:

Source: Fortunly

93% of organisations are considering or have already adopted **cloud services** to reduce privacy concerns

THE SCALERS

3. Assess and engage safe cloud providers

Step 1:

Identify which **cloud providers** your globally distributed team uses. Apart from enterprise-grade providers, your employees may also be using other free file-sharing cloud services.

Step 2:

Migrate all the files of your employees to a **secure provider**.

Step 3:

Review contracts and terms of service to ensure your business **retains ownership** of all the data uploaded to the cloud and that the cloud provider has no right to it.

Step 4:

Ensure that frequent cloud security audits are performed in compliance with standards such as **ISO 27001, PCI, or HIPAA.**

4. Choosing the right partner

And last, but certainly not least, choosing the **right offshore partner** is key.

The right partner will ensure that all cybersecurity measures are in place and tailor security measures based on your **business requirements**.

This allows you to mirror the protocols you use at home and provide **cybersecurity training** modules to all your employees, local and remote.

Conclusion

And that concludes our thoughts on **leveraging cybersecurity** when working with globally distributed teams.

All said and done, a **security breach** could just as likely occur with your local team.

And that's why, implementing bulletproof **security practices** and processes is critical, irrespective of the location of your team.

Thank you

THE SCALERS®

thescalers.com