6 ways to boost your organization's IT security

Security is IT's top priority within tech departments. However, increases in attacks result in cybersecurity nightmares for organizations, and getting on top of security is more important than ever.

1 Get BYOD under control

With the rise of hybrid working environments, employees tend to opt for personal devices, such as laptops and phones, for work. While employees have more freedom and flexibility, IT departments claim unsecured devices are potential security disasters waiting to happen.

The solution is to ensure that 'bring your own device' doesn't get out of hand. Start by setting expectations for your employees. For example, can employees use their phones at work, or are they allowed to download the newest software on their professional devices? Setting boundaries should be clear to all employees before working on personal devices.

2 Use multi-factor authentication

Enforcing multi-factor authentication means users will need to verify their identity, such as by entering a code via a mobile phone number. This means attackers cannot access your organization's data since they cannot enter the company network.

3 Make sure employees are security-savvy

Cybersecurity awareness is not only a job for your IT department but all of your organization. Studies show that 95% of cybersecurity breaches can be traced back to human error.[1] Make sure employees are educated about best practices and what to do if there has been a potential breach.

Train staff to be knowledgeable on specific threats, identify **'spear-phishing'** emails, and how they could potentially impact business. Both IT departments and employees must be proactive and vigilant to cyberattacks. Find out how hybrid working has changed the face of IT security in this blog.

4 Shed some light on shadow IT

Shadow IT refers to all forms of IT that take place outside of and without knowledge and/or approval from the IT department. It also increases the attack surface of the organization, making it more susceptible to things like **data leaks.**

The solution is for IT to partner up with the company's business departments to invest in future-proof solutions. Learn more about shadow IT and how to manage it in this blog.

> **To keep your data safe and sound, it's crucial to build a culture of cybersecurity awareness within your organization.**

TOPdesk

1 Paul Mee and Rico Brandenburg, After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk (WEF, 2020) 1, weforum.org/agenda/2020/

Author: Clementine Jones

Keep security breaches at bay when working remotely

The rise of hybrid working has made managing IT security a whole lot more complicated.

Find out how to manage IT security while employees are working from home in this blog.

5

Back it up, back it up

According to IDC's Ransomware Study, approximately 37% of global organizations were victims of a ransomware attack last year. IT departments need to be proactive, instead of reactive, about ransomware prevention – and recovery.

The solution? Backing up your organization's data. By running regular backups, you'll bypass the ransom demand by restoring data from a source other than the encrypted files. And if you want to prevent malware from encrypting backup files? Use a cloud backup to keep a copy of your files safe from ransomware and other cybersecurity threats.

6

Create a response plan

Creating a comprehensive response plan, identifying key stakeholders, and mapping out the most important processes is the **best way to avoid chaos if the worst does happen.**

For some organizations, responding to a security incident will require collaboration between several departments. By ensuring that all relevant parties agree to their responsibilities in the event of a breach, well before it happens, you can save valuable time and deal with security incidents quickly and efficiently.

Find out how to improve collaboration between departments and which barriers to overcome.