HOSTWAY®

6 Best Practices for Preventing a Security Breach

Are You Protected?

As malicious activity becomes more severe and the frequency of data compromise continues to rise, it’s extremely important to have the right protective measures in place – proactively preventing attacks before they ever begin.

With an understanding of the types of threats that exist and the stages of a breach (see Hostway whitepaper: The 6 Stages of a Malicious Cyber Attack – is Your Business Secure?), businesses can turn an eye toward identifying and bridging gaps in their security strategy.

Best Practices for Preventing a Breach

White it’s best to consult a security specialist as you build your security strategy, the following best practices will help protect your business from some of the most prevalent threats.

1. Adhere To Compliance Requirements:

First and foremost, it’s imperative to follow the guidelines of industry standards such as HIPAA and PCI, including both required and addressable precautions. Compliance is an important step in establishing a robust security posture.

2. Handle Sensitive Data With Care:

HIPAA and other industry security standards require the use of encryption to safeguard sensitive information. Keys of 128-bit strength or higher should be put in place so that even if a malicious individual gains access to a system, they are unable to read the data stored there. Sensitive details like patients’ healthcare information should never be sent via email. A file transfer solution that provides the proper secure access should be leveraged, and only when it is absolutely necessary to transmit sensitive data.

3. Continuous Monitoring:

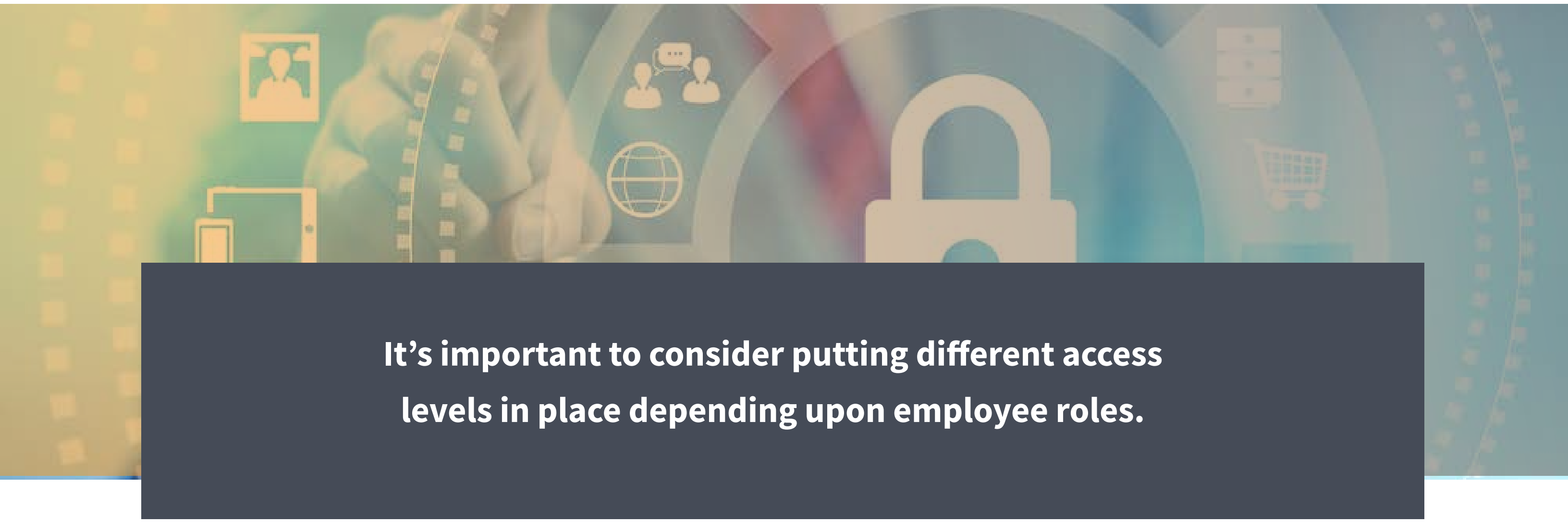
Enterprises in every industry should have a monitoring solution in place that keeps a constant eye on network activities. Monitoring helps identify suspicious activity like that associated with a breach. Once identified, further security measures can be leveraged to prevent intrusion.

4. Dispose Of Data When Possible:

Hackers can't steal what isn't there. While it's sometimes necessary to keep historical information, any outdated assets should be destroyed after a prescribed period of time. What's more, data disposal must be carried out properly to ensure that information is actually eliminated and no longer accessible. Physical files should be shredded, and device drives should be overwritten and completely wiped. Simply deleting files or formatting the drive isn't enough - data can still be resurrected and accessed. When disposing of devices, ensure that the drive is wiped multiple times to make sure that any data previously stored there is illegible.

5. Restrict Access:

When putting authentication controls in place, it's important to consider putting different access levels in place depending upon employee roles. Everyone in an organization likely won't need access to sensitive data - in fact, only those that utilize this information should be granted access to it. This kind of restriction can help combat internal threats and prevent negligence and accidental errors that could open the door to an attacker.



It's important to consider putting different access levels in place depending upon employee roles.

6. Ensure Systems Are Up To Date:

All security patches and updates should be applied to critical systems as soon as possible. These measures help pinpoint and repair any vulnerabilities that an attacker could exploit for a breach. Waiting to put these in place or not updating a system at all can have a severe impact on the overall security posture.

By minimizing attack vectors and blocking unauthorized access, businesses can bolster protection against malicious actors. This process begins with an understanding of the overall threat environment and the risks impacting a company's specific sectors. Through proactive security efforts, enterprises can work to prevent intrusion and reduce the chances of attack.

Trust Hostway with your Security in the Cloud

With over 19 years of cloud hosting experience, Hostway has a rich history of helping industry-leading SaaS and software companies run their mission-critical applications in the cloud. Hostway offers the expertise and infrastructure required to deliver cost-effective, secure, and reliable cloud hosting solutions for a wide range of use cases.

To better understand your company's security exposure and how to mitigate the risk, contact the cloud hosting experts at Hostway for a free risk assessment. We'll help you understand your risk profile and then work with you to design the right cloud hosting solution for your specific requirements.

HOSTWAY®