Top 5 ERP & Work Management Infrastructure Security Risks

BST Global™

If you're an executive at an AEC consultancy or firm, you know that your Enterprise Resource Planning (ERP) and/or work management system is crucial for managing your project portfolios. If your systems are compromised, you risk losing out on project visibility and business forecasting.

To keep your ERP and work management systems secure, we're sharing the top five unnecessary security risks that we see AEC firms take with their system infrastructure. Avoid these common mistakes to ensure that your system stays secure and your bottom line stays strong.

01 Neglecting to Apply Updates to Operating Systems or Applications

The number one risk to an on-premise or cloud-based ERP system is an operating system (OS) or ERP/work management application update that is not applied. Just like with any computer program, when you skip an update for your system, you run the risk of using a less stable and secure version of the software. Not only do software updates improve functionality and add new features, they also strengthen both the security and integrity of your data by patching previous vulnerabilities as new threats are discovered.

OS vendors typically release security patches monthly or off-cycle when a critical vulnerability is found. Meanwhile, ERP/work management vendors release critical updates to currently supported versions of their software only, so ensuring that you use a supported version is key. Avoid using legacy software with little to no security updates, as this decision might come back to haunt you.

It's also critical for your organization to have a patch management process to combat these risks on-premise (or a cloud vendor for the same purposes if the ERP system is SaaS or hosted elsewhere). Stay informed and aware of all new developments in your ERP software and be intentional about how new patches are implemented.

02 Lacking Multi-Factor Authentication (MFA)

It's not enough anymore to have VPNs, strong passwords and password change policies in place. Your organization also needs multi-factor authentication (MFA) in some form. A combination of strong passwords and at least one additional authentication mechanism — such as an authentication application or digital certificate — should be in place for access to your ERP.

Providers like Microsoft, Okta, Duo and Google offer MFA solutions that are easy to deploy and manage. Be careful with text (SMS)-based MFA as numerous vulnerabilities have recently been found with SMS-based solutions.

03 Overlooking Proper Backup & Data-at-Rest Protection (DARP)

Whether your ERP or work management solution is on-premise or in the cloud, your at-rest data and system backups need to be secured. Many recently publicized security incidents involved the theft of unencrypted backup media or physical hard drives which contained business and/or personal data.

To ensure this data is secure, organizations should have a data-at-rest encryption policy in place. This means that all physical media is digitally encrypted to prevent unauthorized use, even if the drives fall into the wrong hands.

Most cloud-based ERP and work management vendors who host their infrastructure on Azure, AWS, Google or other systems provide this type of protection. Organizations that deploy on-premise must typically enable through the OS, database or hardware storage solutions.

04 Disregarding Malware & Ransomware Impacts

The impact of malware and ransomware on an organization's ERP/work management system has been identified as a top risk. Downtime of an ERP/work management system for this type of event can be a few days or even weeks. Losing your ability to manage project portfolios for that amount of time removes major tools from your toolbox, putting a damper on your processes.

Organizations should have comprehensive protection in place for all their endpoints. This includes user workstations, servers and any gateway that allows external access, such as firewalls and data network infrastructure. Cloud-based systems operating on platforms such as Azure and AWS can take advantage of the platform's security services for application protection. Organizations hosting their ERP/work management system on-premises need to rely on their internal Cybersecurity teams to implement sufficient controls.

Most incidents result from insufficient patching and limited cybersecurity awareness training, so training in this area will be crucial to your ERP/work management solution's continued safety.

05 Ignoring Sufficient Disaster Recovery Planning

Disaster recovery planning should include both your organization's infrastructure and business processes. Together, they are known as a business continuity plan.

Organizations should understand both the recovery time during an event as well as any data loss factors. These are known as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

RTO measures how long it takes the systems (or a particular process) to be recovered, and RPO describes any data loss experienced during the event. It is recommended that you work with both your cloud and on-premise teams to establish a service level that your business can agree with. Typically, acceptable RTOs should be between 0 and 8 hours, while RPOs range from 0 to 2 hours. Work closely with your team to ensure that these times remain as low as possible.

Training your team to avoid these mistakes will help bolster your infrastructure security and avoid costly downtime of your ERP/work management system. Stay safe, be prepared and protect your systems today with smarter infrastructure security practices.

BST Global™

About BST Global

BST Global designs, develops and deploys the AEC industry's first suite of AI-powered project intelligence™ solutions specifically for the world's leading architects, engineers and consultancies.

Hello@BSTGlobal.com

BSTGlobal.com