ABC® Associated Builders and Contractors

CYBERSECURITY

# 8 Ways Construction Companies Can Protect Their Mission-Critical Data

## 8 Ways Construction Companies Can Protect Their Mission-Critical Data

By: Neil Jones, Director of Cybersecurity Evangelism at Egnyte

### Data Protection Matters

Once considered mundane administrative tasks, effective data management and protection have become mission-critical to construction companies. This is based upon several factors:

- Increased data. The amount of data created and stored by construction companies has quadrupled over the last four years. And across Egnyte's customer base, AEC firms store more files than any other industry—that's 2.49 times more data than the cross-industry average.
- Costly data breaches. Research from Ponemon Institute shows that the average cost of a data breach has risen to $4.45 million.
- More remote users on jobsites. The construction industry's culture makes it particularly prone to IT risk since employees are often working from various sites, sharing information via unsecured attachments and links, in an environment where administrators can't access users' devices quickly in the event of critical data loss.
- Higher threat of ransomware attacks. Reports show that ransomware attacks are more prevalent for construction firms than for any other industry. There are several ways you can manage ransomware risk more effectively.

### How To Protect Your Data

With the increased importance of data protection to organizations of all sizes, here are eight best practices you can institute right now to maximize your company's data protection.

### Begin With Ransomware Detection and Recovery

If you can focus on only one data protection action in the near-term, consider ransomware detection and recovery. As ransomware demands increased, ransom payouts averaged a whopping $541,010 as of March 2022. To prevent potential ransomware attacks that can encrypt your mission-critical files and stifle organizational productivity, consider a content management platform that detects potential ransomware and flags unusual behavior like high-volume encryption. Many solutions permit you to "roll back" to earlier versions of critical files in the event of a ransomware attack, which is referred to as snapshot recovery. You can read more about the financial impact of ransomware in my recent Quora response.

### Implement Multifactor Authentication

If your IT security budget is limited, another good place to start is with implementation of multifactor authentication. With MFA, users authenticate their access to systems by supplying two or more pieces of evidence—also known as factors. Microsoft research reveals that users who enable MFA on their accounts can block up to 99.99% of automated cyberattack attempts.

### Reduce Content Sprawl

Content sprawl is an issue that's plagued the construction industry in today's era of cloud storage and sharing. Multiple contractors and even employees within the same company operate off of outdated drawings, requests for information, etc., which introduces significant operational and data protection risk. To get started, consider working with a company that summarizes your overall data volume with a convenient portal, so you can reduce the amount of redundant, obsolete and trivial data that your organization manages. This dramatically improves users' productivity, because users have to spend less time searching for the files they need.

To put the magnitude of content sprawl into perspective, Egnyte's Cybersecurity Trends for Mid-Sized Organizations study found that 86% of respondents' organizations manage between six and 15 data repositories. Some examples of data repositories include Egnyte, Microsoft SharePoint and Google Drive.

Meanwhile, a separate Splunk report found that up to 55% of stored data can be considered redundant, obsolete, trivial or dark ("dark data" refers to stale or unused data). So, for every 20 files that an organization stores in its various repositories, only nine of those files can be considered current.

By reducing content sprawl, you not only improve the user experience, you also dramatically reduce an organization's potential cyberattack surface.

**Restrict Users' Access to Sensitive Information**

With so many employees changing positions in the last few years, it's become even more important to restrict users' access to sensitive data. As a rule, general construction project information should be made available to your company's wider user community, but access to highly sensitive data should be restricted only to the files that users need to do their jobs. For example, employees should be able to access their individual payroll information, but most employees shouldn't have access to payroll information for the company as a whole.

Providing complete user access to highly sensitive project details is an accident waiting to happen.

For your reference, here's a real-world example of "need to know" access control guidelines, from the University of California, Berkeley.

**Inventory Your Data Repositories**

As the adage goes, you can't protect data that you can't see. To improve visibility, conduct a comprehensive review and inventory of your current data repository infrastructure. This will help identify potential shadow IT implementations.

In this case, you'll need to combine traditional technological approaches like IT audits and network scanning with in-person outreach. Rather than advocating a "my way or the highway" approach, engage with stakeholders in business units to identify what data repositories they're using regularly, and how the repositories can be secured more effectively. Outreach will also give you important insight into the shortcomings of company-sanctioned data repositories, so you can make your own repositories more effective.

**Restrict File Sharing in Content Collaboration Services**

Content collaboration services like Microsoft Teams and Slack have revolutionized the way that we connect and share content with colleagues and business partners. But such solutions can lead to content sprawl and unsafe content-sharing practices if they aren't managed effectively.

Educate users about the need to share links to files instead of file attachments when collaborating. And when you offboard users, remove their access to content collaboration solutions immediately—such solutions pose significant IT risk and provide an attractive target to potential cyberattacks.

By restricting file sharing in these services, you'll reduce your file storage clutter and improve your security posture.

### Incorporate Data Backup into Your Incident Response Plan

Data backup procedures need to be incorporated into your company's incident response plan. Although that recommendation might sound like common knowledge, one study by continuitycentral.com found that an unbelievable 58% of data backups fail, leaving those companies' data unprotected.

To prevent such situations, your data backup, encryption and business continuity/disaster recovery procedures need to be formally captured in writing and routinely stress-tested. This helps to confirm that data backup processes will function properly in the event of a real emergency.

### Prevent Intrusions Before Attackers Reach Your Data

Another effective way to protect your data is to prevent potential intrusions before they reach your data infrastructure. A comprehensive defense-in-depth strategy combines anti-virus solutions, intrusion detection systems and data encryption with existing data protection processes and MFA. Implemented collectively, that approach will reduce the probability of successful cyberattacks.

If your organization hasn't adopted a robust cybersecurity program, a good place to start is by creating a basic incident response plan that addresses actions your company should take if your mission-critical systems are impacted by a potential data breach.

### To Learn More

For additional insights about data growth and data risk in the construction industry, check out and share Egnyte's AEC Data Insights Report.

## Brought to you by ABC's Tech Alliance Partners

ARCORO®
ExakTime®

AUTODESK
Construction Cloud

BUILDOPS

constructconnect®

EGNYTE

FCA
Field
Control
Analytics

PROCORE®

KPA

KOJO

Sage

smartbuild
Powered With
Microsoft

Smartapp.com™
TURN YOUR JOBSITE INTO A SMARTSITE™

TENNA®

SUBHQ

Trimble