

ABC + EGNYTE

Fortifying Construction:

Strategies for Ransomware Defense and Recovery

www.abc.org | www.egnyte.com | © 2025 by Egnyte Inc. All rights reserved.



Executive Summary

The construction industry is experiencing a significant digital transformation, marked by a dramatic increase in data storage needs and cloud adoption. From 2018 to 2023, the construction segment's cloud storage usage escalated from 0.903 TB to 4.001 TB, reflecting the industry's increasing reliance on digital project management and technology-driven processes.[1] While enhancing efficiency, this digital shift has also exposed construction firms to increased cybersecurity risk, particularly ransomware attacks. Between April 2023 and March 2024, the construction industry was the third most targeted industry sector globally, with 228 reported ransomware victims.[2]

This report provides construction professionals with strategies to fortify their defenses against ransomware and improve their recovery capabilities. Key findings include:

1. 59% of Architecture, Engineering, and Construction (AEC) firms experienced a cybersecurity threat in the past two years.
2. 77% of firms cannot survive more than five days without access to documents before experiencing serious scheduling impacts.[3]
3. The construction industry faces unique cybersecurity challenges due to its increasing reliance on digital technologies, complex operational structures, potential IT constraints, and field-focused resources.[4]

[1]Egnyte's 2024 AEC Data Insights Report
[2]Middle East Business Intelligence, Construction is third most targeted sector by ransomware
[3]Dodge Data, Data Resilience in Design and Construction: How Digital Discipline Builds Stronger Firms
[4]Neuroject, Cybersecurity in Construction; Guide to 2024

Summary of Collaboration Between Egnyte and ABC

Egnyte, a leader in cloud-based data management and security solutions, has partnered with Associated Builders and Contractors (ABC), a national construction industry trade association representing more than 23,000 members, to address the industry's critical cybersecurity needs. This collaboration leverages Egnyte's data management and cybersecurity expertise with ABC's extensive network and industry knowledge to provide comprehensive ransomware defense and recovery strategies tailored to construction firms.

Three critical aspects of this collaboration include:

1. **Industry-Specific Insights:** Combining Egnyte's data from more than 4,000 AEC clients with ABC's deep understanding of the construction industry to provide relevant and actionable cybersecurity recommendations.
2. **Member Education:** Utilizing ABC's platform to disseminate critical information on data management best practices, incident response planning, and recovery strategies to its vast membership base.
3. **Compliance and Governance:** Addressing the high-severity governance issues that are prevalent in the construction segment (60% of occurrences) through tailored guidance and solutions.[1]

By addressing these objectives, the report aims to guide construction firms in fortifying their defenses against ransomware and other cyber threats, ensuring secure and efficient operations in an increasingly data-driven industry landscape.



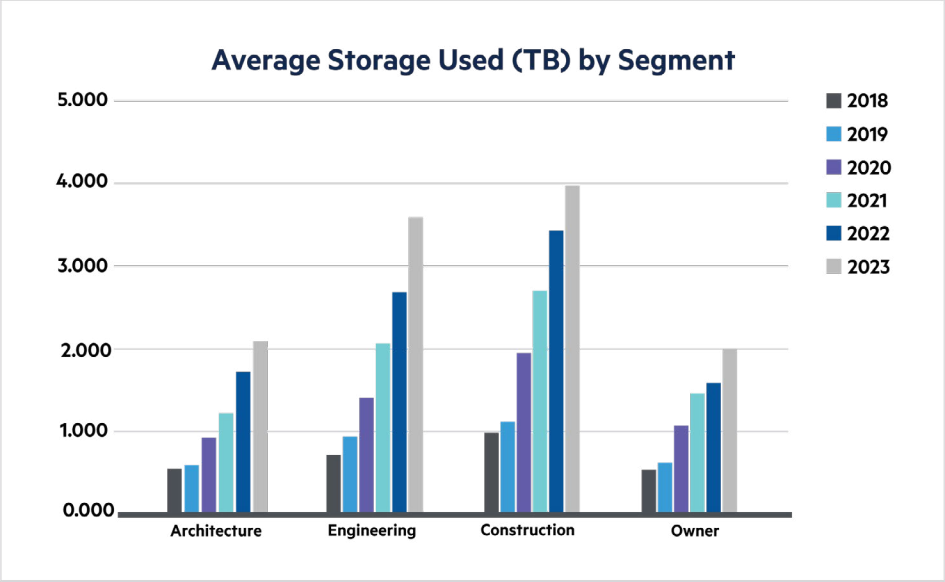


Data Management in Construction

As construction firms increasingly rely on digital tools and cloud-based solutions, they face evolving challenges in managing complex data types, ensuring data accessibility across job sites, and protecting sensitive information from cyber threats. This section explores the current trends and challenges in construction data management, emphasizes the importance of data security, and highlights the industry's prevalent cybersecurity threats. Understanding these aspects is crucial for construction firms to navigate the digital landscape successfully and safeguard their operations against potential risks.

Current Trends and Challenges

The construction industry is experiencing a significant digital transformation, marked by a dramatic surge in cloud storage adoption and an increasing reliance on data-intensive processes. From 2018 to 2023, the construction segment saw cloud storage usage grow from 0.903 TB to 4.001 TB (See Figure 1), reflecting the industry's shift to digital project management and technology-driven processes.[5] This trend necessitates efficient data management practices to handle complex data types and facilitate collaborative project information sharing.



[5]Egnyte's 2024 AEC Data Insights Report

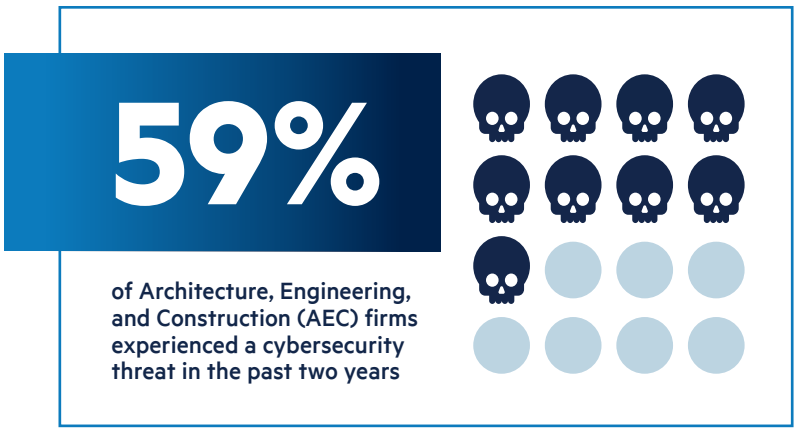
However, this digital shift also presents unique challenges:

1. **Data Volume and Complexity:** The exponential growth in construction data storage purchased underscores the challenge of managing increasingly large and complex datasets.
2. **Accessibility on Job Sites:** Construction projects often face limited bandwidth on job sites, making it difficult for numerous tradespeople to efficiently access and share large files such as detailed drawings, 3D models, and project schedules.
3. **Data Security Risk:** 59% of AEC firms experienced cybersecurity threats in the past two years. The construction segment, in particular, encountered 455,219 high-severity occurrences in 2023, highlighting the urgent need for enhanced cybersecurity measures.
4. **Integration of Multiple Data Sources:** Managing data from various sources, including sensors, drones, BIM software, and project management tools, presents integration and interoperability challenges.

Importance of Data Security

The vulnerabilities in data security within the construction industry are multi-faceted:

1. **Expanding Attack Surface:** Digital transformation has broadened the industry's attack surface, making construction companies targets for cybercriminals. [7]
2. **Supply Chain Vulnerabilities:** The complex network of contractors, suppliers, and partners in construction projects creates potential weak links in cybersecurity.[6]
3. **Outdated Systems:** Many firms rely on legacy software with potentially insufficient security updates, exposing them to known (and unknown) vulnerabilities.[6]
4. **Human Factor:** Employees in the construction industry may lack cybersecurity awareness, making them susceptible to phishing scams and social engineering attacks.[6 8]
5. **Sensitive Data Exposure:** The need for multiple parties to access sensitive project data on job sites increases the risk of data breaches or unauthorized access.



[6]Dodge Data, Data Resilience in Design and Construction: How Digital Discipline Builds Stronger Firms
[7]Neurojet, Innovations in Construction Data Management: Trends to Watch (2024)
[8]Neurojet, Data Management in Construction; 2024 Ultimate Guide

MEMBER STORY

Hensel Phelps:
Protecting Sensitive Project Data

Safeguarding sensitive project data is a critical priority at Hensel Phelps Construction Co., both during a project's lifecycle and after its completion.

The company's security posture at base aligns with the stringent National Institutes of Standards and Technology Special Publication 800-171 (NIST SP 800-171) framework. In particular, Hensel Phelps employs role-based access control with multifactor authentication to ensure that only authorized individuals can connect to project data. The firm securely archives all sensitive data in its project management cloud software, which also adheres to the NIST SP 800-171 framework.

For projects involving controlled unclassified information or other high-sensitivity requirements, data is managed exclusively within a Federal Risk and Authorization Management Program-secure project management system, providing government-grade protection. On-premises data storage is equally secure, featuring immutable solutions to prevent unauthorized data alteration.

Access control for internal staff and external partners is managed per project, following a least privileged access methodology. Each user must have a unique ID and demonstrate a clear business need to access specific information. Single sign-on simplifies authentication for internal users while maintaining robust security. External partners' access is tightly integrated into Hensel Phelps' enterprise application access processes, ensuring seamless and secure collaboration across projects.

Through these comprehensive measures, Hensel Phelps ensures the confidentiality, integrity, and availability of sensitive project data, reinforcing trust and accountability in all their operations.

ABC + EGNYTE

Prevalent Cybersecurity Threats in Construction

The construction industry faces unique cybersecurity challenges due to its increasing reliance on digital technologies and complex operational structures. These challenges include:

1. **Expanding Attack Surface:** The digital transformation of the construction industry, including the adoption of IoT devices, automation, AI, and data analytics, has expanded cybercriminals' potential attack vectors.[9]
2. **Vulnerable Remote Operations:** The proliferation of temporary sites and networks, coupled with a heavy reliance on a temporary workforce, reduces the organization's level of security control while increasing its potential exposure.[4]
3. **Legacy Infrastructure:** Many construction firms operate with outdated IT and OT systems, which may lack crucial security updates and patches.[4 10]
4. **Resource Constraints:** Construction companies often have limited IT resources and budgets dedicated to cybersecurity.[4 5]
5. **Lack of Regulatory Focus:** Historically, the construction industry has not been subject to stringent cybersecurity regulations, which has led to a de-emphasis on cyber priorities.[4]
6. **Sensitive Data Handling:** Construction firms manage large amounts of sensitive data, including financial information, intellectual property, and project designs, making them potential targets for cybercriminals.[11]
7. **Supply Chain Vulnerabilities:** The complex network of contractors, suppliers, and partners in construction projects creates potential weak links that cybercriminals can exploit.[5]

[9]Alliant, Cyber Risk & Security Considerations in the Construction Industry
[10]Curtis, Why Construction Comapnies are Particularly Vulnerable to Cyber Attacks
[11]Capitol Technology University, Combatting Cyber Threats in the Construction Industry

These challenges have contributed to a significant increase in cyberattacks targeting the construction industry. According to recent reports, cyberattacks on construction companies doubled in the first quarter of 2024 compared to the same period in 2023.[12] The construction industry now ranks as one of the most targeted sectors, with an average of 226 incidents per company annually.[13]

MEMBER STORY

Confidential Firm:

Strengthening Cybersecurity in a Remote Work Environment

To adapt to the challenges of remote work and cloud-based operations, a confidential firm has implemented robust cybersecurity measures to protect its corporate network and sensitive data. Remote access is secured through a secure sockets layer VPN with multifactor authentication (MFA), ensuring that only authenticated users can connect. Geo-IP filtering restricts connections to U.S.-based IP addresses to enhance security further, mitigating the risk of unauthorized access from outside the country.

For cloud-based services, the firm enforces MFA policies across all platforms. Additionally, in Microsoft 365, conditional access policies restrict logins to approved countries while automatically addressing risky activities. These proactive measures effectively address potential vulnerabilities in remote and cloud-based workflows.

Recognizing the evolving risks of employees accessing company data from various devices and locations, the firm continually reassesses its approach. To fine-tune its oversight of mobile devices—critical to project management in remote work environments—a mobile device management system is under consideration for the next fiscal year. This step would provide better control of mobile devices, further enhancing the firm's ability to secure its data in an increasingly distributed work environment.

Through its ongoing efforts, the firm is committed to staying ahead of cybersecurity threats while adapting to rapidly evolving work practices.

[12]Cyber Security Review, Cyber Attacks on Construction Firms Jump, New Report Finds
[13]Woodruff Sawyer, Building Defenses Against Cyber Risk in the Construction Sector

Incident Response in Construction

In an era of increasing digital dependency, incident response has become a critical component of risk management for construction firms. This section explores the multi-faceted nature of incident response in the construction industry, addressing its definition, importance, and best practices. We'll examine common types of incidents construction firms face, from data breaches to ransomware attacks, and discuss the role of technology in effective response.

Understanding Incident Response

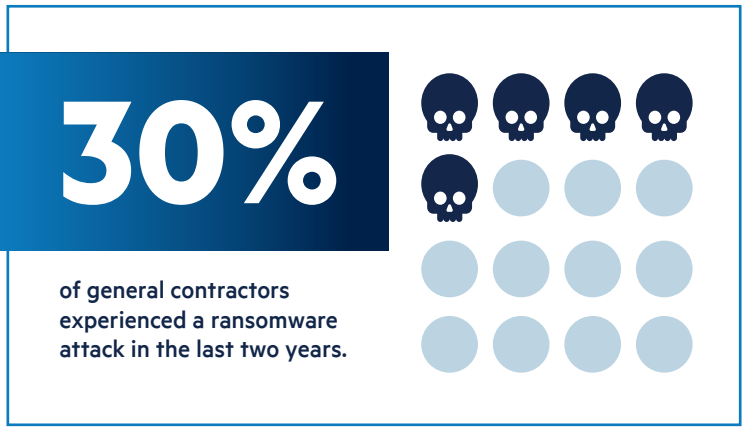
Incident response in the construction industry refers to the process by which organizations handle potential data breaches, cyberattacks, or other security incidents—from initial detection and mitigation to the restoration of systems and everyday operations. The objective of incident response is to contain the issue, limit damage, and decrease recovery time, which is particularly crucial in an industry where project delays can have significant financial and reputational impacts.

According to the Dodge Data report, Data Resilience in Design and Construction: How Digital Discipline Builds Stronger Firms, 59% of firms in the AEC industry experienced a cybersecurity threat in the past two years.[14] This statistic underscores the importance of a robust incident response plan.

Common Types of Incidents in Construction

Construction firms face various types of security incidents that can trigger the execution of a formal incident response plan:

1. **Ransomware attacks:** 30% of general contractors have experienced a ransomware attack in the last two years.[13]
2. **Unauthorized log-in attempts:** This is the most common threat, reported by 45% of contractors.[13]
3. **Unintended third-party access to data:**[15] A significant concern, especially given the complex supply chains in construction projects.[13]
4. **Phishing attacks:** 85% of construction firms experienced phishing attacks in 2023.[13]
5. **Data breaches:** 93% of construction organizations experienced a data breach in the past three years.[13]



[14]Dodge Data, Data Resilience in Design and Construction: How Digital Discipline Builds Stronger Firms
[15]Sharing privileged project data with parties who should not have access is a significant concern.

MEMBER STORY

Gaylor Electric:
Staying Ahead of Cyber Threats

Cybersecurity is a top priority at Gaylor Electric. The company takes a proactive approach to protecting its digital environment through regular user training and awareness programs.

Every quarter, all employees participate in a brief video training module designed to strengthen their ability to identify and handle cyber threats. The training, tracked through the company's learning management system (LMS), includes key lessons on recognizing phishing tactics and general strategies for detecting suspicious activity. Supervisors receive detailed reports to ensure all employees complete their training and address any gaps in participation.

To reinforce these lessons further, Gaylor Electric conducts randomized phishing simulations twice per quarter. These self-phishing emails test employees' ability to identify malicious links or attachments, which can be a precursor for ransomware attacks or malware infection at less security-minded companies. If an employee mistakenly interacts with a simulated phishing email, they are immediately assigned additional, focused training through the LMS. This targeted approach ensures continual learning and strengthens the company's defenses against emerging threats.

By combining frequent, actionable training with real-time phishing simulations, Gaylor Electric ensures its workforce remains vigilant and informed in the face of evolving cybersecurity challenges.

Best Practices for Incident Response Planning

It's essential to have an Incident Response (IR) program in order for your firm to recover from attacks quickly and effectively.

Egnyte's Incident Response Plan outlines six critical components to include in your IR program:

1. **Preparation:**
   - Identify key team members and their roles in the incident response process.
   - Develop and regularly update an incident response plan tailored to the construction industry's unique needs.
   - Conduct regular training and simulations to ensure team readiness. (These simulations are often referred to as "table-top exercises").
2. **Identification:**
   - Implement robust monitoring systems to detect potential security incidents quickly.
   - Train staff to recognize and report suspicious activities or potential breaches and encourage them to "say something if they see something."
3. **Containment:**
   - Establish procedures for isolating affected systems to prevent further damage.
   - Implement measures to preserve evidence for later analysis and potential legal proceedings.
4. **Threat Containment:**
   - Develop protocols for removing threats and restoring systems to a secure state.
   - Ensure procedures are in place to address various types of incidents, from malware to unauthorized access.

5. **Recovery:**
    - Create detailed plans for restoring systems and data, prioritizing critical project-related information.
    - Implement measures to prevent reinfection or recurrence of the incident.
6. **Post-Incident Review:**
    - Conduct thorough analyses of incidents to identify lessons learned and areas of improvement.
    - Update incident response plans and security measures based on those insights.

Role of Technology in Incident Response

Technology plays a crucial role in effective incident response for construction firms:

1. **Cloud-based collaboration solutions:** 55% of users find these highly effective in managing technology risk.[13]
2. **Automated monitoring and alert systems:** These can help detect and respond to incidents more quickly.
3. **Data backup and recovery solutions:** Essential for minimizing data loss and enabling rapid recovery.

Importance of Incident Response in Construction

The construction industry faces unique challenges that make incident response particularly critical:

1. **Project continuity:** 77% of firms cannot survive more than five days without access to documents before experiencing serious scheduling impacts.[13]
2. **Financial impact:** Cybersecurity incidents can lead to significant financial losses due to project delays, data loss, and recovery costs.
3. **Reputational damage:** In an industry built on trust and reliability, security incidents can severely impact a firm's reputation and its future business prospects.
4. **Regulatory compliance:** Many construction projects, especially those in the public sector, have strict cybersecurity requirements (such as CMMC 2.0, for U.S. Department of Defense contractors and subcontractors) that firms must meet.

By implementing comprehensive incident response plans and leveraging appropriate technologies, you can significantly enhance your resilience against cyber threats and minimize the impact of security incidents on your operations and projects.



Recovery Strategies for Construction Firms

As cyber threats grow, robust recovery strategies have become essential for construction firms to ensure business continuity and minimize the impact of potential incidents. This section explores the key components of a comprehensive recovery plan and provides actionable recommendations for construction firms to enhance their resilience against cyber threats. From implementing robust data backup and storage solutions to leveraging cloud-based technologies and improving their incident response program, these strategies help construction companies quickly recover from disruptions and maintain their competitive edge in a digitally driven industry landscape.

Key Components of a Robust Data Recovery Plan

1. **Data Backup and Storage:**
    - Implement localized and cloud-based backup solutions.
    - An effective data backup and storage strategy is imperative to keep up with rapidly expanding data volume.
    - 99% of architects and 91% of engineers back up their documents as a mitigation strategy.[15]
2. **Regular Testing:**
    - Conduct frequent tests of the recovery plan to ensure its effectiveness.
    - Only 39% of AEC firms believe they have a high degree of preparation when considering the potential loss of access to key documents.[15]
3. **Incident Response Team:**
    - Form a dedicated team responsible for executing the recovery plan.
    - Define clear roles and responsibilities for each team member.
4. **Communication Protocol:**
    - Establish a clear communication plan for internal staff, clients, and stakeholders, including regular updates.
    - 53% of architects and 54% of engineers are concerned about negative impacts on company's reputation due to cyber incidents.[15]
5. **Technology Integration:**
    - Leverage cloud-based collaboration solutions, which 55% of users find highly effective in managing technology risk.[15]
    - Implement automated monitoring and alert systems for rapid incident detection.

Recommendations For Your Firm

The AEC industry has long demonstrated its resilience and ability to overcome challenges, adapting to operational and technical hurdles with ingenuity and persistence. By implementing the following strategies, construction firms can fortify their cybersecurity posture, ensuring the continuity and resilience needed to thrive in today's evolving threat landscape.

1. **Prioritize Cloud Adoption:** Given the expanding volume of cyber threats and the disparate data access that characterizes the AEC industry, your firms should accelerate your transition to cloud-based solutions for improved data resilience and accessibility.
2. **Enhance Cybersecurity Measures:** With 59% of firms experiencing cybersecurity threats, implement robust security protocols, including multi-factor authentication and regular security audits.
3. **Improve Document Access:** Focus on technologies that enable access to documents anytime, anywhere, and on any device. Currently, only 39% of firms report high access to documents.[16]
4. **Invest in Employee Training:** Develop comprehensive cybersecurity awareness programs to address the human factor in security breaches. Gamify the awareness sessions to make them more engaging and increase retention of the training content. Consider offering small prizes (such as gift cards) for your employees who accurately report cyber threats.
5. **Implement Regular Backups:** Follow the lead of architects and engineers who overwhelmingly back up their documents as a primary mitigation strategy.
6. **Business Continuity & Disaster Recovery (BCDR):** Consider implementing BCDR solutions to ensure rapid recovery and minimize downtime.[17]
7. **Conduct Regular Risk Assessments:** Continuously evaluate and update the recovery plan based on evolving threats and business needs.
8. **Strengthen Supply Chain Security:** Given the complex nature of construction projects, develop security protocols for data exchange with external parties.[18]

By implementing these strategies and recommendations, construction firms can significantly enhance their resilience against cyber threats and maintain business continuity in the face of potential disruptions.

[16]Dodge Data, Data Resilience in Design and Construction: How Digital Discipline Builds Stronger Firms
[17]Egnyte, What is Business Continuity



Conclusion

The construction industry stands at a critical juncture in its digital transformation journey, facing unprecedented opportunities to improve data management, cybersecurity protections, and workforce resilience. As the AEC Data Insights Report reveals, the industry has experienced a dramatic surge in data storage needs. This exponential growth underscores the urgent need for robust data management practices and enhanced cybersecurity measures.

As the construction industry evolves, embracing digital technologies and fostering a culture of innovation will be crucial for building resilience against cyber threats and other business risks. By implementing the recommendations outlined in this report, construction firms can strengthen their defenses, improve operational efficiency, and position themselves for success in an increasingly digital landscape.

The path forward requires a concerted effort from all stakeholders in the AEC industry to prioritize data resilience, cybersecurity, and technological advancement. The construction sector can protect itself against current threats and lay the foundation for a more secure, efficient, and innovative future.

Contact Us

Egnyte, Inc.
US: 1.877.734.6983
EMEA-UK: +44.20.3356.3714
www.egnyte.com

ABC + EGNYTE