Managing Risk in the Construction Industry

There was a time when managing risk in the construction industry had more to do with accounting for bricks, mortar, and pickup trucks than securing tablets, laptops, and smart phones. Insuring the company truck was more critical than ensuring all digital plans and assets were secure in the cloud or datacenter. Whether you're a small specialty contractor or a large general builder, making sure adequate security procedures are in place has never been more complex.

With blueprints taking a backseat to digital plans and construction software correcting errors and balancing the budget, many contractors, sub-contractors, and estimators are left reeling when it comes to effectively addressing the inherent risk in this technological revolution. Complicating matters is the danger of hiring and retaining enough skilled workers in a robust, high-demand economy. Not only is there a shortage of skilled labor, the workforce is aging with 20 to 24-year-old workers making up only around 7 percent of the workforce, down from 11 percent a decade ago, according to Construction Executive magazine. Having to hire outside a company's comfort zone can also impact productivity levels and run up risk levels.

> Today's construction landscape is facing a perfect storm of managing people and processes.

Simply put, today's construction landscape is facing a perfect storm of managing people and processes, alongside visible and invisible assets. In the decade since the dawn of the iPhone, these issues have grown exponentially. Companies are not only spending hundreds of thousands of dollars on physical field equipment, but also on technology, which cannot necessarily be chained, locked, and hoisted 100 feet in the air.

Pinpointing Vulnerabilities

As the construction industry has matured, managing risk has become more than just about making sure your project is on-time and on-budget. Some companies simply don't grasp the potential impact of allowing the office estimator to also serve as the resident IT expert. With or without a dedicated IT person or department, companies often move forward with a false sense of security. Even when they don't want to be in the business of managing data, they still try to do it themselves, rather than opt for the very affordable cloud datacenter. Are these companies really factoring in the harm that could be done from one power outage, fire, laptop theft, or misplaced mobile phone? Probably not.

The irony is that you have to look no further than a mobile or wireless device connected by Wi-Fi and a cell tower to find a company's most valuable, and vulnerable, assets and intellectual property. The convenience of accessing data at your fingertips – including client lists, contact names, past projects, and bid information – is coupled with the danger of disclosure. Failing to adequately safeguard and secure these inter-connected assets and the software that manages it all could leave a contractor facing the unthinkable – having to rebuild their database from scratch. For example, a project manager might have three levels of proprietary information on their smart phone – their company's information, their client's information, and maybe even data from a client's client. These out-of-sight, out-of-mind assets need to be top of mind when assessing risk and taking the necessary steps to protect against loss and liability.

While the beauty of the digital world is that it allows companies to seamlessly collaborate with clients and suppliers, it also leaves plenty of room for human error when swapping digital plans and change orders back-and-forth. The spread of mobile technology and BYOD (bring you own device) programs mean it is not uncommon to access and share digital drawings beyond office walls – whether it be in the field, the cab of a truck, or from an at-home office. As a result, this tends to increase a company's exposure to potential breaches and theft. These vulnerabilities mean construction firms must implement policies and processes, extending security across the work site and the office to ensure protection of both physical and intellectual assets.

Step-by-Step Process to Reduce Risk

Put simply, companies should plan for the worst when striving to manage and reduce risk. A positive first step is to adopt a three-part approach made up of 1. Assessment, 2. Mitigation, and 3. Monitoring and Reporting.

Step 1 – Assessment This first step can be quite a hurdle for smaller firms of 25 or less employees. Taking stock of what data types a firm collects and maintains, as well as where it is stored and secured, can be eye-opening. This process helps construction firms identify and evaluate vulnerabilities and potential areas of exposure to the business, whether the risk is physical, intellectual, or technological.

Where to begin? Working with current employees, companies should review business processes, such as auditing the existing administrative policies, adequately training employees, and reviewing security oversight processes. Contractors may know to implement some level of computer access security, such as procedures for passwords, backup and recovery, and network virus/malware protection. Often, this focus is centered on the external theft or attack, but what if the unthinkable occurs – the theft or attack originates from the inside?

Companies should plan for the worst when striving to manage and reduce risk.

Step 2 – Mitigation Following an assessment of business practices and technologies, companies can move on to mitigation. This refers to developing risk management procedures that will proactively reduce and eliminate vulnerabilities on an ongoing basis. Putting an IT administrator in charge of password administration is a great starting point for many companies. Even training everyone to follow a posted checklist that reminds the last person out the door to back up the tape drive can be a huge leap forward for smaller firms.

Clearly, human error can be reduced by enforcing policy and training. However, if construction firms outsource their policy manual, they should make sure it doesn't gather dust on a shelf for 15 years. This is why transitioning institutional knowledge is so important. Construction firms should never allow one lead person to own all of their risk management processes.

Step 3 - Monitoring and Reporting Assessment and Mitigation need to be supported and sustained by Monitoring and Reporting policies that are conducted on a regular, scheduled basis and are under constant review. Having safeguards in place will ensure companies are alerted to any potential discrepancies, breaches, or dangers. For example, are passwords changed when employees leave? Does the contractor know who is accessing the applications that house their contacts and their projects? If people walk out the door with copies of the software, can they still use it even after they are no longer employed by the company?

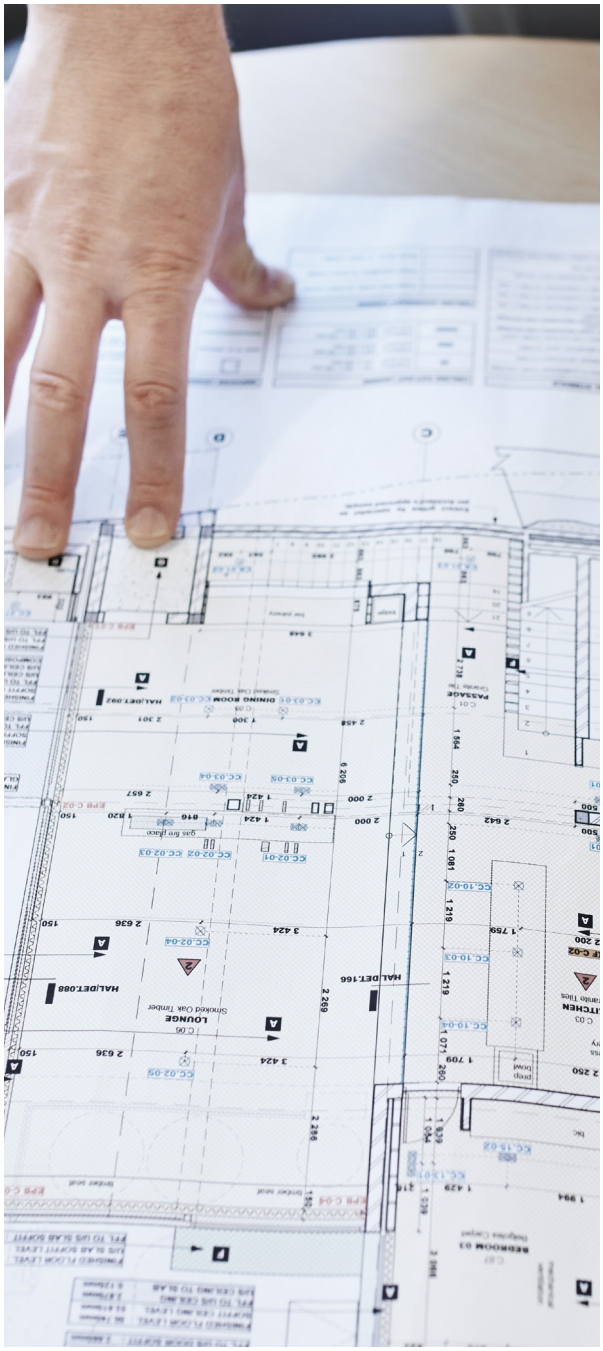
Even better, how does a firm handle common mistakes? For example, consider the case of an estimator marking up drawings at home and forgetting to upload the information or copying the wrong drawings or documents. Losing 200 to 300 pages of drawings could set a firm back multiple days if they don't have good policies in place to ensure all work is securely backed-up and easily accessible.

Overcoming Hurdles and Challenges

For many firms, having the right policies and training in place does not necessarily result in less exposure. Paying to have your estimators trained on construction software and having a robust database doesn't necessarily fix the issue when it comes to disaster recovery or hacking. Firms that invest heavily in their database often fail to ensure that it is backed up securely. Consider the issue of allowing multiple estimators to have wide-ranging log-in rights with little password enforcement. This is why it is essential to enforce database processes, password protection, and restrict access levels.

When it comes to implementing risk management procedures, many contractors are turning to automation technology like digital estimating tools and project management software. This technology can lock down tools, information, and assets while helping to improve productivity and profitability. As a result, transferring information in real-time between laptops, PCs, tablets, and smartphones make it much easier to access and share sensitive documents anywhere, at any time, with any one. Unfortunately, the realities of an on-the-go workforce also make it much easier for intellectual property theft to occur from inside the business when transferring time and labor documents, as well as plan changes to accommodate client demands.

In fact, insider attacks can be costlier or more damaging than outsider attacks, according to the 2016 State of Cybercrime survey of 400 U.S. organizations. Nearly half (47%) of survey respondents felt that electronic crimes perpetrated by insiders were costlier. With a growing awareness of this issue, how can contractors implement management strategies to secure information, processes, and property without micromanaging, or frustrating, their employees?



Implementing Controls to Drive Up Productivity

When it comes to implementing rules around technology, some firms may find it difficult to enforce consequences.

Most companies can agree that they want to protect their assets and drive up productivity while mitigating frustration and risk. This can be tricky when deploying both manual procedures and automated solutions that can access and track information about data usage in real time. When firms have accountability and oversight, they can know, not guess, whether employees and data are in the office or at a remote site. Being able to precisely pinpoint who is using what information, with which applications, and on what device is critical to mitigating any unintended exposure.

When it comes to implementing rules around technology, some firms may find it difficult to enforce consequences. For example, if a project manager is handling proprietary data and using their smartphone camera to copy this information, they should face consequences for potentially exposing company information.

While on-site equipment has long been protected with physical locks and site barriers during off-hours, firms can now use secure badges and swipe cards. Many construction firms are looking for even more granular data to track employee movements for greater visibility into their productivity. For example, to combat timecard cheating, some construction firms use thumbprint and, in some cases, facial recognition to reduce the risk of labor fraud.

While on-site equipment has long been protected with physical locks and site barriers during off-hours, firms can now use secure badges and swipe cards.

Building a Strong Defense for Everyone's Benefit

In this hyper-connected world, having a mature plan for cybersecurity is key to preparing a strong defense. With internal controls in place and employees trained to mitigate risks, automated construction software can help firms answer the question of who is doing what, what information is being used, and which devices are being used in the process. Risk management safeguards can protect both physical and intellectual property, including sensitive business information and plans for new products and/or services. Ultimately, this can benefit all participants – owners, employees, and clients.

The stakes are clearly high. Consider the increase in "spear phishing" attacks where bid information is stolen when an attacker targets a company by impersonating a key employee or known associate in an email. A recipient can be tricked into opening a malware-infected attachment or visiting a malicious website. Construction companies are not the only entities at risk when a breach occurs. Client information is also vulnerable. Hackers seek personal information on customers and employees to use or sell or they may try to leverage a company's access to its business partners' confidential business information, intellectual property ,or plans and specifications. Risk management will protect clients' data and influence their future business decisions, including who they contract within the future.

Planning and preparation are the keys to a strong defense, ensuring that adequate internal controls are in place and employees are trained to recognize and respond to threats. In an increasingly inter-connected marketplace, the importance of a robust, mature cybersecurity program simply cannot be understated. For example, how long would a contractor be a preferred bidder if they experienced a highly publicized breach? By implementing controls, construction firms can safeguard and boost their own reputation among clients and the industry.

As technology advances and competition increases, having an active risk management plan in place will only become more necessary for construction firms. Selecting the right construction software and tools is essential to ensure contractors can quickly and easily monitor who is accessing plans, bids, and projects for a safe and secure growth plan.

On Center Software is a trusted, established, and growing construction software company developing on-premise and Software as a Service (SaaS) takeoff, estimating, and production management solutions from their office in the The Woodlands, TX. For nearly 30 years, On Center Software has stayed focused on helping estimators win more bids and turn winning bids into profitable projects. Today, the company boasts more than 40,000 users in more than 60 countries and their products are taught at more than 300 universities and institutions.