BLUEBEAM
A NEMETSCHEK COMPANY

Applied Software
GRAITEC Group

Data Security in Construction:

The Time To Act Is Now

The construction industry has become a top target for cybercriminals all over the world. Here's why construction companies need to bolster their defenses—and how they can get started.

The time to act is now

With the world becoming increasingly digital, cybersecurity has emerged as one of the most critical elements of every organization's business strategy. As of 2021, the global cybersecurity market stood at $185 billion, according to a report by Grand View Research, with the industry expected to grow 12% compounded annually from 2022 to 2030.

Central to the rise and rapid growth of the cybersecurity industry is the ever-evolving role data plays in the global economy. With more of the world connected by internet technologies, data has become the critical commodity harvested by companies and governments to optimize everything from major public policy down to the consumer decisions people make every day. The Economist even went as far as to suggest that data is now the world's most valuable resource—not oil, which for centuries has served as the most significant and sought-after commodity in the world.

The construction industry has ridden this datafication wave as well. Digital technologies have taken over construction, architecture and engineering just as they have every other sector. Software has been the primary tool digitizing construction, as previously paper-based construction plan document creation, management and review processes have gone digital, allowing industry stakeholders to collaborate more efficiently and complete projects faster and within budgets.

Another report by Grand View Research pegged the global construction and design software market at $9.6 billion in 2021; it's expected to compound at an annual growth rate of 8.5% from 2022 to 2030.

Such growth in digital technologies—and, by extension, data—in the construction industry comes with significant cybersecurity risks.

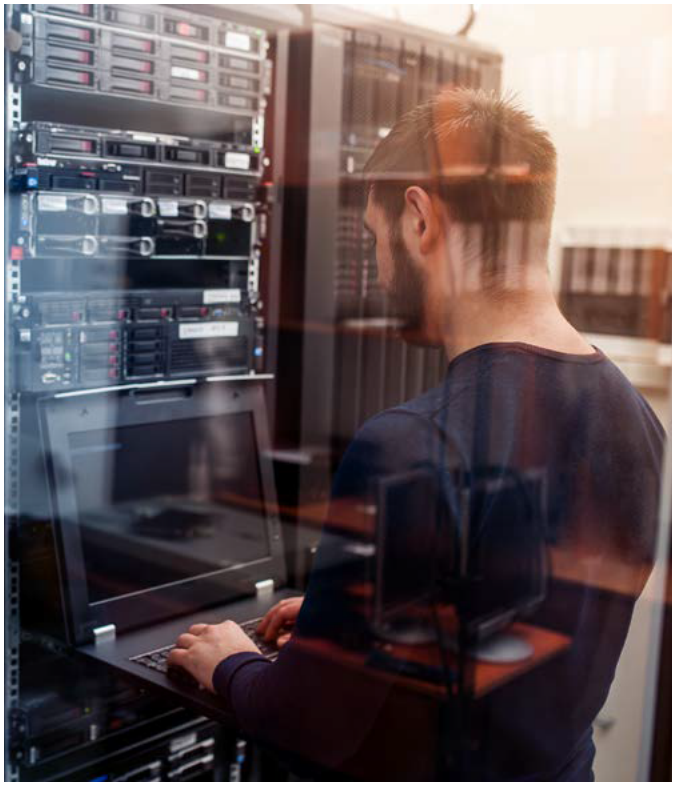
Hackers intent on breaching organizations' data systems and extorting them for significant dollar amounts are increasingly keen on targeting the construction industry. In fact, in 2021 construction was the No. 1 industry hit by ransomware attacks, a hacker-induced computer virus that holds a device hostage until the owner pays a fee to regain access. Such attacks have harmed construction organizations both large and small, as smaller firms are less likely to have cybersecurity measures in place. The cumulative financial losses because of cyberattacks can cost the industry billions of dollars annually, according to a report in Construction Dive.

Cybersecurity 101

Cybersecurity, at its most basic definition, is the art of protecting networks, devices and data from unauthorized access or criminal use, and the practice of ensuring confidentiality, integrity and availability of information, according to the Cybersecurity & Infrastructure Security Agency. There are several diverse ways organizations should conceptualize their cybersecurity efforts.

Network Security

This is being able to protect data from unauthorized users via an organization's computer network. It includes an organization's firewall, email security, antivirus measures, anti-malware security and data loss prevention.



Information Security

This element protects an organization's critical business information from destruction, disruption and alteration. It includes an organization's cloud security, cryptography, vulnerability management and incident response.

End-User Behavior

This component ensures an organization's end-users—its employees, contractors, etc.—are properly educated and knowledgeable on the individual actions and behaviors needed for security best practices. This education includes knowledge of the several types of cyber threats, including phishing scams, as well as actions required to guard against such threats, like device security, password creation and physical device security.

Infrastructure Security

Finally, this consideration is meant to protect critical information from corruption, sabotage or terrorism. It includes aspects such as network infrastructure, data center protection and security, as well as managing power, cooling systems and water supplies for these physical assets.

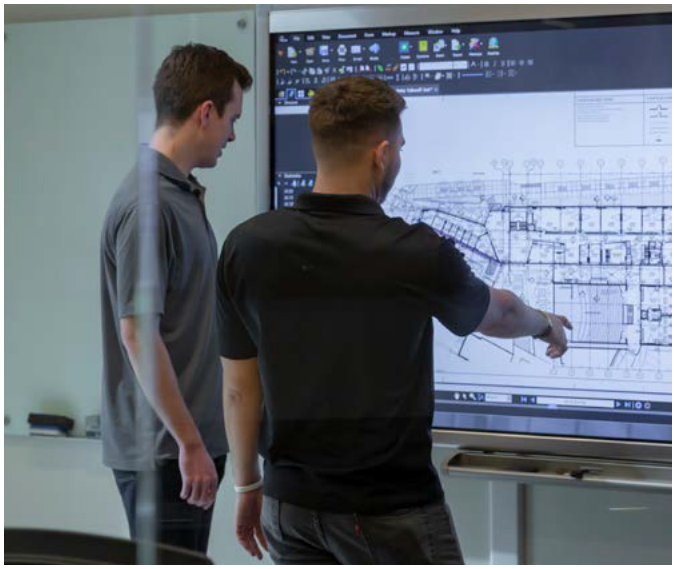
To ensure construction organizations are as protected as possible from cyberthreats, it's critical that their defenses include each of these cybersecurity elements. Unfortunately, however, the industry is far behind on cybersecurity. As a result, the construction industry has become a top target for hackers, who have a successful history of breaching companies' data.

Notable recent hacks

Several recent high-profile construction industry cyberattacks highlight the urgent need for firms to bolster their cyber defenses.

In January 2020, French contractor Bouygues fell victim to a ransomware attack that temporarily shut down and cut off some of its critical computer systems, the company announced at the time. The Maze ransomware gang claimed responsibility for the attack; the group publicly posted online a 1.2 gigabyte file containing vital Bouygues data.

The attack came just days after Maze struck another construction firm, Canadian contractor Bird. It remains unclear from published news reports if either breached company paid the hackers to regain access to their data, or the extent to which each company's operations were adversely affected.



The following May, in two separate incidents, two UK-based hospital construction companies, Bam Construct and Interserve, were each targeted by a cyberattack that shut down some of each company's computer systems. It's also unclear from published news reports if either company suffered any long-term operational damage, or if they gave in to hackers' demands to retrieve access to their data and systems.

Lastly, after Russia invaded Ukraine in February 2022, Construction Dive reported of increased warnings that Russian-led cyberattacks were poised to specifically target construction industry firms.

It doesn't appear that any specific Russian-led attacks on construction firms have been publicized to date. Each of these incidents should put construction leaders on notice. The time to focus on and drastically improve data security infrastructure is now.

Why construction is a top hacker target

The construction industry is unique. Every project—whether it's building a skyscraper, erecting a bridge or expanding a complex highway system—requires a vast network of loosely connected stakeholders to complete. While this reality comes with many positives, there are some aspects to this structure that make the industry especially vulnerable to cyberattacks.

The following are the primary reasons construction has become a top target for hackers:

Slow to transition to digital

Today's construction industry is awash in digital technology, but compared to other industries its adoption has come much later. Some of the reasons the industry has been slow to adopt technology are, coincidently, many of the same reasons that hackers are now most interested in targeting construction firms. Even though the industry has come a long way in its embrace of technology, construction still spends about 80% less of its revenue on information technology when compared to other industries, according to Construction Executive. The industry's reluctance to adopt digital technology means it has also been slow when it comes to data and cybersecurity, making it a prime target for hackers.

Operates with a distributed work environment

Every construction project involves many separate entities—developers and financiers, general contractors, engineering and architecture firms, specialty subcontractors, government agencies—all working together sharing critical project information and executing financial transactions across disparate networks with few, if any, shared security protections. There's no singular corporate firewall, for instance, guarding against the potential for breaches.

Each contractor has their own technology, processes, etc., for their individual businesses; every time they engage with another project entity's technology or process, they are potentially creating an opening for hackers to jump in and steal critical information or data.

Processes many transactions

Because of the messy nature of separate stakeholders involved in each construction project, there's lots of money changing hands all the time. In addition, there is a significant variety in payment amounts. There can also be many payees involved on a project, as larger builds may require hundreds of small individual specialty contractors.

Taken together, these construction industry characteristics make it especially at risk to cyberattacks. As a result, hackers have been known to use this disconnected security network to spoof, phish and often directly steal money from industry stakeholders by effectively re-routing money to their own criminal accounts. Hackers are most likely to target their efforts, experts say, at times when workers and systems have their guards down—say, a Friday afternoon, when workers are tired from the long and busy week and looking forward to their weekend activities. This is when a delicately planned phishing email or payment re-routing is likely to arrive, hopeful that the person in charge of administering such a routine transaction or payment isn't being vigilant.

And because the industry still operates using simple invoicing systems, it's easy for hackers to pose as vendors or subcontractors requesting their scheduled payments.

Fewer regulations and compliance concerns compared to other industries

Finally, construction is among the top targets for hackers because it's one of the least regulated when it comes to data protection and security. Government efforts to regulate cybersecurity and data privacy have been focused elsewhere, particularly in more consumer-oriented sectors like social media and other fast-evolving consumer technology subsectors.

How construction firms can secure their data, bolster overall cybersecurity

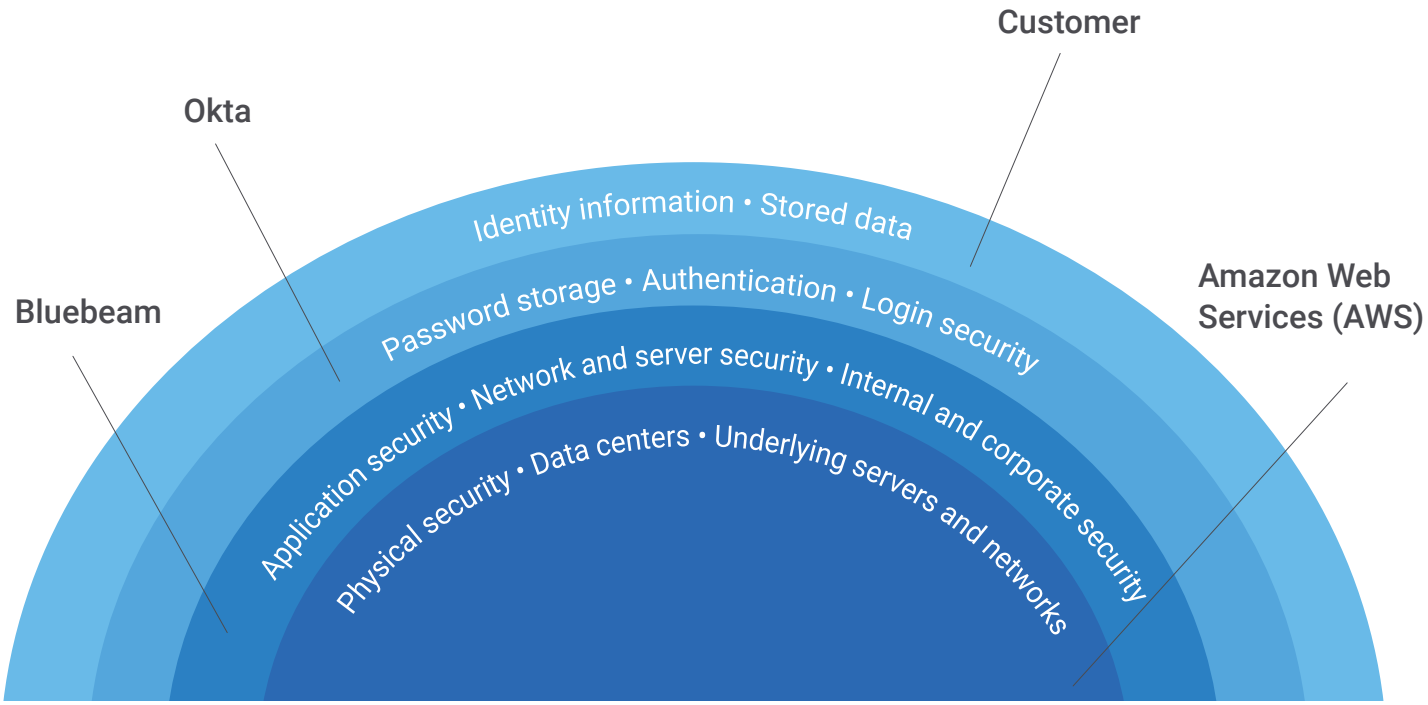
Fashioning a strong, comprehensive cybersecurity effort isn't easy. It requires an incredibly disciplined and complex security posture where responsibility and accountability are shared not just up and down an organization's hierarchy but across to the technology providers a company decides to work with, as well as other external, third-party entities involved at every level of a construction project.

Additionally, as construction's cybersecurity vulnerability becomes more widely known, it's likely that governments around the world will enact more industry-targeted regulations.

The shared responsibility model

At Bluebeam, we advocate for a shared responsibility model when it comes to construction cybersecurity. This means that several stakeholders must be involved to make cyber defenses as protective and effective as possible. Together, their collective protection measures offer the most secure defenses against the evolving threat of cybercriminals.

The following construction industry stakeholders have important roles to play to enact a collective cybersecurity response.



Third-party cybersecurity providers

Every firm that aims to bolster its data security needs is likely to partner with an outside cybersecurity provider for help with services such as password storage, authentication or login security. To this end, it's paramount that these external cybersecurity providers have their own defenses and protocols in place, and that construction firms are diligent in vetting the firms they partner with on this front.

Technology providers/partners

Any time a construction organization acquires or engages in a license or subscription to a new piece of technology or software, it's essential that these technology providers have also taken the appropriate measures to ensure their products are compliant and equipped to safeguard their customers' data. Every technology provider must have its own application security, network and server security and internal corporate security.

Contractors or other construction firms

First and foremost, construction organizations themselves must take cybersecurity seriously. It's not a "nice to have"—it's a must have.

There are several ways to do this, but most critical is taking steps to ensure that their identity information and stored data systems are protected and secure. It's also essential that construction firms take a leading role in vetting the extent to which all their outside business partners and vendors are protected from cyberthreats. Lastly, construction firms have the responsibility to ensure that their employees are all educated in the individual measures they are required to take to keep their own—and the organization's—data secure. Knowing how to write effective and secure passwords, using virtual private networks (VPN) and secure Wi-Fi networks for sensitive projects and engaging with multi-factor authentication protocols, for instance, are all imperative actions on the part of a company's employees.

Cloud computing providers/partners

With the proliferation of cloud computing and storage, every business nowadays engages with a third-party cloud provider such as Amazon Web Services (AWS), Microsoft Azure, IBM Cloud or Google, among others. These companies build large physical data centers all over the world, allowing their customers access to reliable and cheap data storage and exchange services without having to house expensive on-premise servers of their own.

Not only do individual construction organizations engage with these cloud computer providers themselves, but so do their technology application partners and cybersecurity vendors. As a result, it's pivotal that, in addition to a company's own cyber-threat defenses and those of its technology and data security providers, these large, enterprise cloud providers have their cybersecurity in order as well.

They primarily can do this by focusing on the physical security of their millions of square feet of data center facilities, and making sure that their underlying servers and networks are following the evolving set of government regulations focused on data security.

Forging ahead

The construction industry is inarguably one of the most important sectors in the global economy. The buildings, homes, infrastructure and other associated structures it produces are central to human life on earth and a functioning and civilized society.

As such, it's increasingly critical that as the world—and the construction industry—continues to become more interconnected through the proliferation of data and the technologies that allow for its efficient transfer and use, the industry takes a leading role in protecting itself and its stakeholders from the serious threats posed by cybercriminals. The risk of inaction is simply too great to ignore.

About Bluebeam Inc.

Trusted by over 2.4 million individuals in morethan 165 countries, Bluebeam's smart, intuitive solutions advance the way technical professionals work, manage and collaborate on projects digitally. Founded in 2002 in Pasadena, CA, Bluebeam has grown to include additional offices in California, Texas, Illinois, Germany, England, Denmark, Sweden and Australia. Bluebeam is part of the Nemetschek Group.

Next Steps

Learn how our global data infrastructure helps organizations mitigate risk and stay compliant with superior security, privacy and control.

FIND OUT MORE

Try Bluebeam with a 30-day free trial.

See what Bluebeam can do for you team.

START YOUR FREE TRIAL

Applied Software
GRAITEC Group

BLUEBEAM®
A NEMETSCHEK COMPANY