EGNYTE

State of Ransomware Report for Architecture, Engineering and Construction

Research, Analytics, and Insights from over 2,700 Egnyte AEC Customers

Introduction

As the threat, scope, and impact of ransomware continues to grow, organizations across every industry are acutely aware of the increasing likelihood of an attack. But amid a deluge of media and industry reports sounding the alarm, what are the real chances of falling victim to an attack and what will be the implications for your organization? And do those chances and negative impacts differ by industry?

This report analyzes reported ransomware incidents among Egnyte's Architecture, Engineering & Construction (AEC) industry customers. While the attacks were not due to any vulnerabilities in the Egnyte platform and Egnyte customers are seeing a much lower incidence of attacks than publicly available sources, this research paper looks to gain additional insight by comparing the rate of successful ransomware attacks on our AEC companies versus all other industries. It also evaluates specific insights and implications from those attacks and outlines best practices that AEC companies should implement immediately to mitigate the chance and impact of a ransomware attack.

> "The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location.
> *(June 2, 2021)*
>
> **- Anne Neuberger |** Deputy National Security Advisor for Cyber & Emerging Technology"

Compliance and Security Are Not Just for Large Enterprises

- AEC companies were **more than twice as likely** to be the target of ransomware than other customers in the sample.
- Companies with **over 1,000 employees** were at the highest risk of attack..
- The overwhelming majority of attacks were against companies in **North America**.
- The median number of files impacted by an attack was **18,800**.
- Egnyte customers can expect an **average of 6.5 days** from support ticket open to support ticket close after a breach is identified and reported, compared with the **global average of 23 days**.
- **More than 31%** of the companies that were victims of ransomware were successfully attacked at least once more within a 16-month period, and a small number were attacked more than twice.

Industry Benchmarks

While finding a definitive stat that indicates how much ransomware is on the rise can be difficult, all indications point to the number of attacks increasing quickly. The FBI's 2020 Internet Crime Report stated that the number of reported ransomware incidents rose from **2,047** in 2019 to **2,474** in 2020[1] and Cybersecurity Ventures predicted that in 2021 a business will be attacked by ransomware **every 11 seconds**[2]. Analysis by the Safety Detectives, Ransomware Facts, Trends and Statistics 2020 highlighted that in the past year the percentage of companies across the major industries that reported ransomware attacks was anywhere from 4.6% in the financial industry to 15.4% in Government, with Construction reporting at 13.2% . It is important to note that Egnyte is seeing a **much lower rate of reported attack across all our domains** at 1.16% across all industries and especially construction and engineering firms at 2.4% (see point 5).

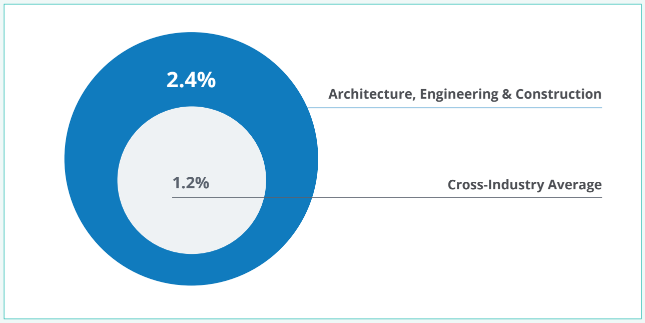
Egnyte Research Findings

Below are **six key findings** from the anonymized data, and analysis of those outcomes.

1. AEC Companies Were More than Twice as Likely to Face a Ransomware Attack

Findings

- Within the study cohort, **28%** of the total number of ransomware attacks detected were in the AEC industry, compared to **72%** for all other industries combined. Even though AEC is Egnyte's largest vertical, this still equates to 2x the number of reported attacks versus the average number across all other industries.



Analysis

- AEC firms have several factors working against them that may lead to a higher rate of targeting. They are very schedule driven and any delays due to lack of access to their files will significantly impact their costs and damage their brand. Couple that with low profit margins, and AEC firms may be more likely to pay a ransom to get up and running more quickly than other industries.

- In addition, AEC firms (and especially construction firms) have a very large attack surface due to a significant portion of their workers being remote. Many also maintain a shared information environment with a myriad of subcontractors, which opens them to additional entry points. Lastly, pockets of the AEC industry tend to lag behind other industries in both awareness of, and defense against cybersecurity threats.

[1] FBI 2020 Internet Crime Report

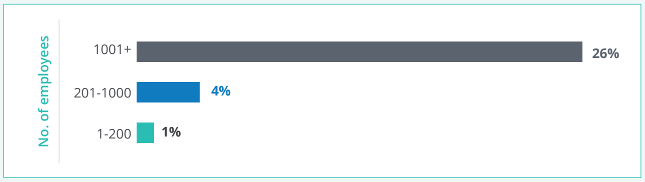
[2] Cybersecurity Ventures - Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021

[3] The Safety Detectives: Ransomware Facts, Trends and Statistics 2020

2. Large Companies Are Most at Risk

Findings

- Ransomware incidents in the AEC industry are most prevalent in large companies, with over a quarter (**26%**) of accounts reporting a successful ransomware attack. This is compared to only **1%** of accounts in companies with less than 200 employees and **4%** of accounts in companies with between 201 and 1000 employees.



Analysis

- This trend is likely driven by opportunity and return on effort. Larger firms, which have over 1,000 employees, benefit from more advanced cybersecurity awareness and resources, but they also have deeper pockets, which make them a more attractive target for bad actors looking to cash in on a large return. These firms also have a lot more data and a lot more repositories, which increases the number of potential entry points and vulnerabilities.

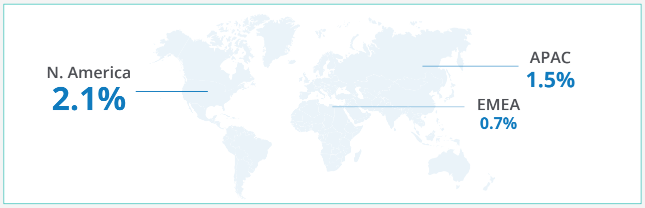
3. North America Makes Up the Vast Majority of Reported Attacks

Findings

- There is a disproportionate prevalence of attacks in North American AEC companies, with **2.1%** of domains reporting a successful attack. This is in direct comparison to **1.5%** of accounts in APAC and **0.7%** of accounts in EMEA reporting a ransomware breach.

Analysis

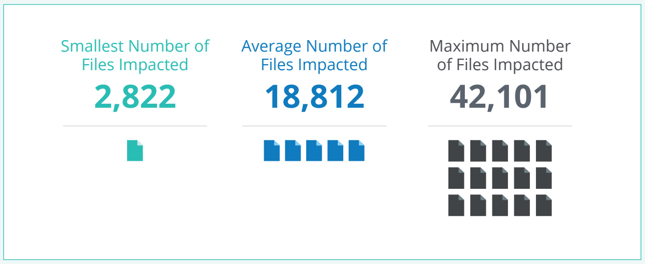
- Ransomware attackers go where the money is, and North America is fertile hunting grounds when targeting companies with deep pockets and a willingness to pay.



4. The Number of Files Impacted Varies Greatly by Occurrence

Findings

- The damage to an AEC company's operations by a successful ransomware attack is dependent on how many files are impacted and the criticality of those files. Therefore, it is important to understand how many files could be impacted prior to the ransomware being identified and contained. We found on average that **18,812** files were impacted by an attack, with the minimum number being **2,822** and the maximum being **42,101**. For scale, it's important to understand that some Egnyte customers have hundreds of millions of files stored on our service, so in many cases the damage was limited in relative terms.



Analysis

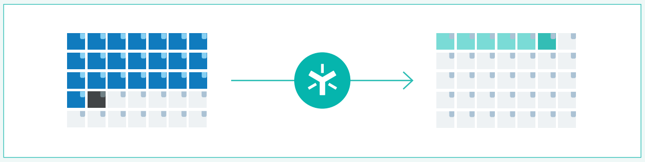
- There are numerous factors that go into how successful a ransomware attack is and how many files are ultimately impacted, some of which are driven by the attackers and some of which are dictated by the victim. It is important to note that the goal of ransomware is to enter the system and spread as quickly as possible to encrypt the maximum number of files. Therefore, the power, effectiveness, and infection vector of where the ransomware is deployed is a big contributor to how many files are infected and how fast.

- From the attacker's point of view the success of an attack is judged squarely on whether they can extort money from the victim, and how much. Therefore, from the victim's side, the cybersecurity applications and how up to date they are, the accessibility of individual files, and detection time are major factors that determine how far the ransomware can penetrate before it is contained. The true impact of an attack goes beyond just paying the ransom, if the company chooses to do so, but also must include operational outages, total downtime and any reputational damage that may occur.

5. The Average Resolution Time After a Breach Was Identified

Findings

- The average time for an Egnyte AEC company to have the issues resolved (i.e. the time from when a support ticket is opened until it is closed) is 155 hours. While in many cases the firm can access their data much quicker, on average the company can expect some level of disruption to operations for **6.5 days**. Globally, the average downtime due to ransomware is between **15 and 23 days**[4], depending on industry, company size, and other factors.



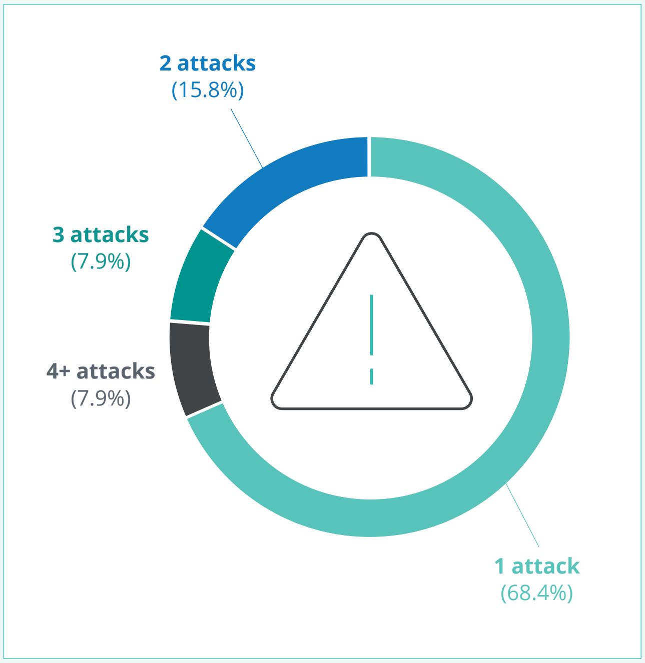
Analysis

- The total time it takes to resolve the issue depends on several variables, which is why the industry range of recovery time can be anywhere from a few hours to a few months, with most companies reporting an average of between one and two weeks. For Egnyte clients specifically, the length of time is calculated from ticket open to ticket close (including some administrative overhead) depends on both the client and the severity of the attack. And even though companies can expect a significant disruption there are several best practices that can be leveraged to greatly reduce the time to recover, including proper trash deletion policies, content retention policies, and version management policies.

6. Repeat Victims: Companies That Are a Victim of a Ransomware Attack Get Hit Again

Findings

- Of accounts that reported an attack, a third (**31.6%**) of them were impacted **more than once** with a small percentage (**7.9%**), reporting four or more incidents in a 16.5 month period.



Analysis

- There could be several factors that lead to a second successful attack on a given account, such as a continuing opportunity, reinfection (where either two individuals initiate a breach by clicking on the same phishing email or the ransomware lies dormant only to be activated at a later date) or ransomware selling. In the case of continuing opportunity, once a threat actor is successful, they may continue to exploit an account until that infection vector is closed or vulnerabilities are patched. Ransomware selling, seen commonly as ransomware as a service (RaaS), is when a successful attack methodology is sold to another attacker who then employs it again. RaaS employs a subscription-based model that enables affiliates to use already-developed ransomware tools to execute attacks. Because of its simplicity, the user does not need to be a proficient coder, allowing even rudimentary individuals or organizations to execute sophisticated attacks. It is interesting to note that one Egnyte customer was attacked a total of 6 times within the study's 16 month time period. Having been successfully attacked once should be regarded as a risk factor for subsequent attacks.

- As demonstrated in this section the threat and impact of ransomware to AEC companies remains high. Being such a prime target means companies need to do everything in their power to prevent and, in the case of a successful ransomware attack, quickly recover before it severely impacts their operations, brand reputation, and the bottom line.

[4] Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound, April 26, 2021, Coveware

A Primer on Ransomware Protection

While there is no 100% guarantee for avoiding a ransomware breach, an organization can implement several best practices to reduce the impact to operations and cost. When looking at best practices, it is best to break it down into 3 phases: identification, containment, and eradication.

Identification

The faster a ransomware attack can be identified, the easier it is to limit the damage it can do to the organization's files. That is why all AEC firms should implement preventative and automated detection capabilities such as:

- Ensuring they are running up-to-date endpoint detection response to continually monitor and respond to cyber threats.
- Establishing an identity access management solution to limit access to specific technologies and files.
- Employing a next-gen firewall and zero-day threat detection to intercept first-of-a-kind attacks.
- Implementing unusual behavior detection to identify anomalies that could be a ransomware attack.

Containment

Once a successful attack has been detected the organization needs to move quickly to stop its self-replicating properties and restrict its access to targeted files. This can be realized in two streams, restricting the ransomware's access to files and restricting the users' access to files by:

- Ensuring that the trash purge policy is adjusted based on requirements. Egnyte recommends at least 30 days after deletion of data.
- Implementing a codified file version policy. Best practice is to retain at least three versions.
- Setting a reasonable content retention or lifecycle policy.
- Implementing script blocking functionality to restrict the use of cookies.
- Installing automatic ransomware notification so administrators can cut off user access in case of a breach.

Eradication

When an attack is contained, the next step is to eliminate it from the system by purging any potentially infected files and replacing them with a clean backup. This requires predetermined actions as part of a complete disaster recovery plan, such as:

- Backing up all data with a third-party cloud vendor.
- Enabling selective file restoration to reduce downtime.
- Establishing a vetting process for both employees and equipment to reduce the chance of reinfection.
- Creating a clean network to run operations until you are sure all ransomware has been eliminated.

The final, and most important best practice to prevent ransomware is education. Today, 85% of all breaches involved a human element[5]; which includes phishing, business email compromise, lost or stolen credentials, using insecure credentials, human error, and misuse. And while those will never be eliminated (people are human), education can significantly reduce the likelihood of them occurring. A comprehensive cybersecurity awareness program, formalized, updated, and delivered to all employees on a regular basis will go a long way to preventing a successful ransomware attack.

[5] DARKReading - 85% of Data Breaches Involve Human Interaction: Verizon DBIR. https://beta.darkreading.com/operations/85-of-data-breaches-involve-human-interaction-verizon-dbir

Conclusion

The threat of ransomware continues to rise as economic and technological factors make AEC firms prime targets for bad actors. The only way to stem this increase in attacks is to make it unprofitable to criminals by making it either too difficult to breach the network, through both active defense and employee education, or by not paying the ransom and thus denying them a return. But it requires forethought, planning and diligence to both harden the network and have secure backup to replace the files rather than paying the ransom. As the saying goes: there are two types of companies, those who have been attacked and those that will be attacked. A comprehensive program that starts by looking at the most critical content is required to prepare for a ransomware attack so the firm can mitigate the impact and get operations up and running as soon as possible.

As the saying goes, there are two types of companies: those who have been attacked and those that will be attacked.

> Making ransomware unprofitable is effectively the only way, short of a coordinated global regulation of cryptocurrencies, to stop these criminals.
>
> **- Anne Josephine Wolff |** Assistant Professor of Cybersecurity Policy, Tufts University

Study Methodology

This study was conducted specifically to determine the impact of ransomware on the Egnyte AEC customer base. To understand our methodology we have outlined our approach and called out specific notes below.

Approach

1. The data range was from January 1, 2020 – May 14, 2021.
2. Data was collated, anonymized, and analyzed by Egnyte's Data Analytics Team.
3. Insights and analysis was developed by Egnyte's AEC Industry Experts and Governance Experts.
4. This study considered all Egnyte customers who had a ransomware incident when comparing the overall occurrence of attacks. We only considered AEC customers for all other analysis.
5. The study counts only those ransomware attacks that impacted the Egnyte repository based on support tickets during the defined date range with a specific focus on AEC customers. Companies may have sustained additional ransomware attacks on other systems.
6. Industry statistic were gathered from a variety of sources and are all cited.

Notes

- The Construction industry represents the biggest segment of the Egnyte customer base.
- The identity of companies that experienced a breach will always remain undisclosed without their expressed permission.
- The quote from Josephine Wolff came from "Ransomware Sentiment After a Summer of Headlines, by Bill Siegel on October 8, 2019 on Security Boulevard, https://securityboulevard.com/author/bill-siegel/

Schedule a Meeting Today

EGNYTE

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs. For more information, visit **www.egnyte.com.**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com