EQUIPMENT WORLD
BY RANDALL REILLY

Getty Images

BUSINESS

Cybersecurity for Contractors, Part 2: What To Do When You're Attacked

Unless you have your data backed up where the cyber-criminals cannot get to it, you will likely have to pay the ransom. But it can be negotiated.

By — Tom Jackson

Jul 14th, 2022

In the last few years, cybersecurity has become a big issue in the construction world. Contractors are vulnerable and easily targeted by hackers, with ransoms and work stoppages costing millions of dollars.

In Part 1 of this series, we discussed why construction companies are so frequently targeted by cyber-attacks. In this article, we'll show you what to do when you are attacked and how to set up a cybersecurity program for your company that will help prevent these attacks.

When disaster strikes

If you haven't hired a cybersecurity consultant before you get hit with an attack, you will definitely need one when you do. A probable course of action a consultant would take would look something like this:

- Create an incident response plan.
- Identify the threat.
- Find the holes in your defenses
- Plug the leak/remove the virus.
- Identify additional weaknesses and fix those.
- Then negotiate to reduce the ransom

Negotiating with criminals

Source: Nick Espinosa

Unless you have your data backed up where the cyber-criminals cannot get to it, you're likely going to have to pay the ransom. But it can be negotiated.

"I have yet to pay full price for ransom," says Nick Espinosa, chief security fanatic at the cybersecurity firm Security Fanatics. "Last year we had an AEC (architecture, engineering and construction) firm, get hit with a ransom for $5 million, and we got it down to $1.2 million. I had a small mechanical contractor get hit for $85,000 We got them down to $10,000. So you can negotiate these things."

Negotiations often give cybersecurity contractors time to figure out the hack, plug the holes and rebuild the system as well, says Espinosa. And once the system is more secure, there is more incentive for the hackers to lower their demands. “There's an entire methodology we use and it makes for some interesting conversations,” he says.

Hacker tech support

After a ransom has been negotiated and paid, hackers will usually restore your data—but not always perfectly. “You might get your Word documents back, Excel files, PDFs and photos, but databases are tricky,” says Espinosa. “They are easy to break, so some of these big files are not recoverable, or recovering them may take a lot of work.”

Reporting compliance

There is no standard set of laws for notifying law enforcement or other agencies after you have experienced a cyber-attack. However, depending on the work you do, you may have to let different agencies know. For example:

- If you experience damages or pay a ransom, you’ll have to notify your insurance company.
- If you are a business that takes credit cards, there is a reporting requirement.
- If you are a business doing work for the Department of Defense or the federal government, the FBI may need to be notified.
- If you are a publicly traded company you may need to notify the SEC, or the Federal Trade Commission.

State and local officials may also have shield laws and privacy laws which protect consumers. Regulations typically require you to notify any customer whose email or other data may have also been breached. “My recommendation is to check with your state and local jurisdictions because you never know what laws you’re going to fall under,” says Espinosa.

How to establish a cybersecurity program

To defend your company against cyber-attacks, understand one thing. A complete cybersecurity defense is not something your IT department or IT person (assuming you have one) can usually provide.

Cybersecurity and IT are two different animals. Espinosa says that people who do this kind of work have different educations and credentials. Most networked systems for home, office or field come with a minimum level of security, but to build a firewall against attacks requires an entirely new layer of protection on top of your IT and network system.

Training for everybody

“First and foremost, all of your people need training,” says Espinosa. “This is the biggest problem we have in cybersecurity. Everybody needs to learn, from the janitor to the CEO.”

Along with training, cybersecurity companies will update your systems, firewalls, and wireless access points. They will also fix potential vulnerabilities that are known and can be exploited and set up encryption systems for your data. Understand also that protecting your company from cyber-attacks is not a one-time fix.

Hackers are always inventing new techniques. Anti-virus software goes out of date. New or untrained employees, vendors or subcontractors start using your system. And all these scenarios bring new risks. Cyber security has to become a part of your company culture, with constant vigilance, much like safety culture.

Backup plans

By far, the most critical part of your defense is to have all your data backed up, either to the cloud or a remote server that you control that is not plugged into the internet, or both.

“I can't tell you how many times I've seen the cloud or cloud backup pull a company out of the fire,” says Espinosa. Even if hackers aren’t a threat, backups can protect your data against floods, fires and other natural disasters, making this a no-brainer for every company.

The cloud services provided by Amazon, Apple and Google are typically well hardened against attacks. Unless you set up your cloud services wrong, hackers should not be able to attack these.

Time and cost

Establishing a cyber-secure operating environment for your company is not cheap, nor can it be done quickly. Six-figure costs are the low end of this kind of consulting work and seven figures are common. Analysis of your company’s vulnerabilities can take up to six months.

But for this, you should get things like firewalls, spam filters, anti-virus programs, training, an annual vulnerability assessment, and penetration test, and data backup plans.

In evaluating cyber consultants look for companies whose people have certifications such as Certified Information Security Manager and Certified Business Continuity Professional. Also, seek out providers who are members of the Information Systems Audit and Control Association (ISACA) and the Disaster Recovery Institute International (DRII).

There are also two governing standards to pay attention to:

- ISO/IEC27001 is an international standard for information security.
- NIST 801-171 is a federal standard for contractors working for a federal agency.

Government work

The Department of Defense also has a standard in the works that will become law in the next year or two that will directly affect construction contractors doing business with certain federal agencies, the CMMC 2.0. You may have heard about the original CMMC 1.0, which had a troublesome rollout. It's not law yet, but it is being retooled to be easier and less cumbersome for contractors.

Two things to note about CMMC 2.0:

1. In the near future, you won't be able to bid on Department of Defense jobs unless you've had an audit and you meet the standards.
2. It is anticipated the CMMC standards will eventually cover all federal agencies and will likely be adopted by states, counties and municipalities, meaning you won't be able to do any public work without certification.

In Part 3 of this series, we will detail what you need to know to get your company ready for CMMC 2.0 audits and certification.

Nick Espinosa *is a cybersecurity expert and founder of Security Fanatics. As the co-author of the bestselling cybersecurity book "Easy Prey," a TEDx Speaker and the host of The Deep Dive nationally syndicated radio show he has given presentations on this subject to numerous construction associations.*

Espinosa contributed to the creation of the National Security Administration's certified curriculum to help the cybersecurity/cyberwarfare community to defend our government, people and corporations from cyber threats globally. He is also a member of the Forbes Technology Council, and a frequent contributor to that magazine's website.

Source URL: https://www.equipmentworld.com/business/article/15293874/cybersecurity-for-contractors-what-to-do-when-you-are-attacked