Berkley Construction Professional
a Berkley Company

Prepared for Berkley CP by
KROLL

The Cybersecurity Risk Outlook: Construction Contractors

Alan Brill, Senior Managing Director, Cyber Risk, Kroll

Cybersecurity, and more particularly failures in cybersecurity, have been in the news throughout the pandemic. Cyber criminal actors have been busy. Whether they are exploiting previously unrecognized vulnerabilities in the software we use (like the February 2021 cases relating to four vulnerabilities discovered in Microsoft's Exchange email servers), or exploiting human weaknesses with phishing campaigns or business email compromises, the risks to data and money are greater than ever. A recent case in which hackers gained access to a water treatment plant and tried to increase the level of lye in the water supply could have succeeded had a plant operator not noticed that his mouse cursor was moving—and that he wasn't the one moving it.

In addition, there has been an increase in ransomware attacks in which criminals or nation-state actors target organizations, as well as significant concerns tied to internet of things devices. These threats may lead you to realize that your organization lacks cyber security personnel and training—and why construction companies have become desirable targets for cyber criminals.

While construction companies' contractual relationships and complex supply chains make them prime targets for cyber criminals, they can be attacked for many reasons. Using the Exchange vulnerability as an example, perpetrators were able to scan large number of systems across the internet to identify the Exchange servers that had not protected themselves by running the "patches" provided by Microsoft and remained vulnerable to the attack methodologies. The very fact that they were running software that was discovered by the hackers to have a previously unknown vulnerability was enough to turn them into a prime target.

What's also significant – and a fact that has received less publicity – is that running the security patch should immunize the system from future attacks (at least those using the newly discovered vulnerability) but running the patch does not tell you if you were already compromised before you could install the patch. To identify those intrusions, a forensic examination to look for specific indicators of compromise that will likely be found in the server is needed.

At Kroll, we get front row seats when we help organizations deal with incidents. We serve as investigators and forensic scientists who can work through logs and sort out the digital "breadcrumbs" that many cyber-attacks leave behind. We work with law firms and with insurers who specialize in cyber-related issues.

© 2022 Kroll. All Rights Reserved.

We can track intrusions to understand how they worked and what they targeted. We can work with clients to identify software implanted in a network to provide the cyber criminals with the ability to continue an attack even when they have been detected and the victim company thinks the incident has concluded.

As a result of dealing with thousands of actual and suspected incidents, helping companies plan and carry out defensive plans and providing training, we can draw some informed conclusions on the kinds of problems that those in the architectural and engineering communities are most likely to encounter.

Certainly, any kind of attack could occur, but our experience tells us that the following risks are the most likely to materialize.

Ransomware

The Problem

This is a form of malware that typically introduces itself to you by displaying a screen indicating that the files on your computer have been encrypted, and that the only way to regain access is by sending the criminal a payment, often in bitcoin or another virtual currency. There are warnings that without the payment, the files will never be recovered (mostly true, although free decryption systems have been developed for some variants of ransomware) and if the ransom is not paid by a certain deadline, you will never get a decryption key—or that the price for getting the key will start going up the longer you wait.

What is particularly scary is that in about half of the cases we investigate through digital forensics, before encrypting the software, the criminal copied the stolen data to a site they control. They can then add the threat that they will release the data if you don't pay the ransom, and you will face a data breach on top of the ransomware encryption. Of course, they promise that if you pay the ransom, not only will you get a decryption key, but they will erase every copy of your data that they hold. The truth is, if the forensic analysis indicates that your data was stolen, and if that data is sensitive, you already have a potentially reportable data breach. Experience indicates that in many cases, if you don't pay, they will post some or all of your data on dark web "shaming sites" or sell it on the dark web. In addition, if you get a decryption key, it may not work, or may only work for a portion of the files, with a second payment demanded for a key that will give you access to all of your data.

Some of the cyber-criminals running these malware campaigns are very organized. We have seen instances where the malware provides detailed instructions for obtaining the virtual currency they insist on as their form of payment and how to transfer it the criminal's online digital "wallet." We have even seen one version that is so sophisticated that the cyber criminals ran a "help desk" a victim could call for assistance in paying the ransom. Because the calls used voice over internet protocol, they could not be traced to a physical location.

© 2022 Kroll. All Rights Reserved.

One additional issue that has come up in dealing with ransomware is the possibility that a ransom payment—most often to a criminal in an undisclosed location—may violate national laws regarding financial sanctions and restrictions on payments. There is no exception to sanctions laws for "we were just paying a ransom" and violations of sanctions laws can carry significant penalties on top of all the other costs associated with ransomware.

What to Do

Unfortunately, many forms of ransomware, once they infect a system, encrypt files in an unbreakable way. While paying the ransom (which the FBI does not recommend) might get a decryption key, the most important defense is one of the oldest—having backup copies of files. Remember, however, that some ransomware is very sophisticated and tries to find backups so that it can encrypt them, too. Some ransomware operators, once they have gained access to your systems, may carry out reconnaissance to determine how to maximize the damage that will be inflicted when they launch the encryption. This includes trying to locate backup files that can be accessed by traversing your network. Many varieties of ransomware can spread the infection through a company network, so rather than dealing with one computer with its files encrypted, the company finds itself having to deal with hundreds or thousands of disabled machines.

When ransomware first appeared, the ransoms demanded tended to be in the low hundreds of dollars. Criminals now demand ransoms in the tens or hundreds of thousands of dollars to unlock all of the computers in an enterprise, and a number of cases have been reported with ransom demands in the millions of dollars. As noted, whether the payment will result in a working key is or destruction of stolen data is something of an unanswerable question. Getting help quickly is vital, both to reduce the spread of the infection and to manage the forensic investigation. This is an area where it is vital to coordinate with your legal counsel, risk manager and insurance broker (where there are cyber insurance claim considerations) as well at your technology team. While ransomware attacks are common across industries and government agencies, they hit individual businesses infrequently, so it is likely that an internal team will have very little experience dealing with ransomware attacks or their aftermaths.

For contractors, their complex supply and business partner chains can make things even more complicated. For example, the hack into Target's network was traced to an account used by the heating, ventilation and air conditioning contractor who managed environmental issues in Target's facilities. The criminals were able to escalate their privileges and transit from the HVAC systems to the financial systems and place malware into point-of-sale devices. It is extremely important to make sure that you restrict third-party access to only the necessary minimum. Placing sensor software (called "agents") into both servers and end-user computers and having those sensors monitored continuously for indicators of compromise has become a best practice. Endpoint sensors can be easily installed and tied into the networks of highly experienced monitoring services which employ technical experts who have the breadth of experience to recognize problems at an early stage, and who have access to indicators of compromise (IOCs) which can provide both early warnings of intrusions and proof that an intrusion occurred. This is a case where having professional monitoring through the internet can provide protection that would likely be unavailable to a typical construction companies (while the largest corporate and government organizations can afford to establish and staff a security operations monitoring center in-house).

© 2022 Kroll. All Rights Reserved.

Malware Affecting Insufficiently Patched Systems

The Problem

Malware—hostile programs developed by governments, criminals, cyber-terrorists and activists—is based on vulnerabilities. These are the "holes" that the bad program can exploit to attack the target. Some of these, called "zero day" attacks, are unknown to the developers but are discovered by the attackers. The vulnerabilities found in Microsoft Exchange in early 2021, and in SolarWinds in 2020, are examples of previously unknown and unrecognized vulnerabilities that the criminals (whether commercial hackers or nation-state actors seeking intelligence data or data to help their own nation's organizations) can exploit.

As vulnerabilities are discovered, software developers will frequently issue "patches" which are software updates that eliminate or control a vulnerability. Vulnerability data is published and is available to anyone. While it might at first seem like attacking a known vulnerability for which a working patch has been issued would be a waste of a hacker's time, it isn't. A patch, no matter how effective, only works if it has been properly installed, and sometimes they aren't. In one case, we determined that an attack that caused significant problems for a financial institution was successful because it exploited a weakness that a patch had been issued for more than two years earlier. However, the patch was never applied to the bank's systems, so the vulnerability remained, and they were hit by an automated attack that was searching for systems that were unpatched. An investigation showed that the person responsible for patching the systems had been on leave at the time it was issued and did not install it upon their return. This problem could have been easily remedied had the bank regularly run a vulnerability scanning program which analyzes an organization's software and detects whether all appropriate patches have been applied.

In another case, a construction company's systems were compromised by stealthy malware that constituted an advanced persistent attack (APT) which enabled the perpetrators to remain inside the target organization for an extended period, probably measured in years. During that time, they were able to exfiltrate sensitive information on projects being proposed, including costing and bid data that were very useful to international competitors. The company did not detect the intrusion until they were notified by law enforcement agencies that had been investigating foreign intrusions into domestic corporations.

What to Do

The simple answer is "apply patches," but there are potential complications. In some organizations, there may be equipment connected to a network that can be affected by a patch. This is particularly true of internet of things devices, which will be discussed below.

A related problem is using an operating system or specialized software that can't be patched. We find that many organizations are running operating systems that are no longer receiving security patches

© 2022 Kroll. All Rights Reserved.

(such as old versions of Windows). For most software, manufacturers announce an "end of life" date after which they will no longer develop or provide patches to resolve operational or security issues. If your organization is running obsolete software, recognize that you are operating in great danger. Unless there is a specific reason (for example, connection to a device that requires that you use the obsolete software), you really shouldn't be using it. If you absolutely must use it, you should isolate the at-risk system from the internet (and perhaps from most of your in-house network) to mitigate risk.

Business Email Compromise Attacks

The Problem

This is an issue that may be of particular importance to construction companies. Contractors receive payments and then disburse funds to suppliers and subcontractors.

We have seen a significant increase in business email compromise (BEC) attacks.

In a BEC, an attacker sends an email message (or often a series of messages) instructing an employee—often a mid-level accounting or finance staffer—to send a large wire transfer to a specified account at a specified bank. The story given is that this is part of a very secret acquisition or a requirement that has suddenly materialized or simply explaining that the supplier has changed banks. The message purports to be from the CEO or another senior executive. The attacker often does the research needed to know that the person purportedly sending the message is traveling (perhaps to speak at a conference) so cannot easily be reached to confirm the email. The email also states that the CEO puts great trust in the recipient to get this done and to keep the request confidential.

Unfortunately, all too many of these succeed, and in some of these cases, it becomes impossible to reclaim all or part of the money transferred. Some cases have involved losses of millions of dollars. A careful look at the BEC emails often shows them to be fake. They originate from an email domain very similar—but not identical—to the real domain. But sometimes, if email inboxes have been compromised by the attacker, the emails might originate from the stated system.

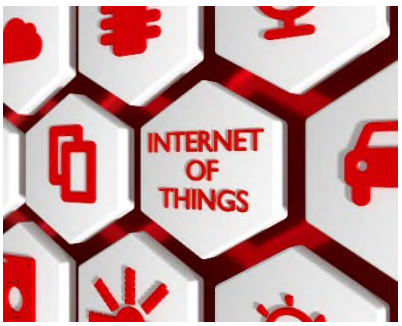
What to Do

Recognize the problem and speak to those who handle your organization's financial transactions like wire transfers. Tell them that if they ever get an email requesting an unusual transfer, to not carry it out unless they can verify it by phone. If you can't rule out the need to potentially send an emergency transfer when you're not able to personally validate it, consider the use of a special code. Choose a phrase that you can remember. Write it on a piece of paper and seal it in an envelope. Have it placed in a company safe by a senior official you trust. Then, if you send an actual request, they should respond by saying "Prove who you are." You would respond with the code phrase, which an outside attacker wouldn't have. The envelope is opened to verify the code. Tell your team to ignore any transfer order where you don't send that phrase, no matter how urgent the email appears to be.

© 2022 Kroll. All Rights Reserved.

Internet of Things – Devices

The Problem



As more and more devices are connected to the internet, security researchers have discovered that some of these devices have little or no security, and that in some cases, hackers can use them for various purposes. They may use them as a point of attack to gain entry into your network. They may want to control the devices, or use them to attack third parties or earn money by "mining" cryptocurrencies like bitcoin. Some devices have passwords that are published and cannot be changed. Others cannot have security problems fixed because they were not designed to be updated.

What to Do

Contractors who specify, source or install connected devices should check the products they are considering and determine whether they present security problems that may make them less suitable than alternative items. Additionally, consider taking an inventory of devices you and your clients already use to determine if there are devices known to have security risks that cannot be effectively mitigated.

Attacks against Your Data Stored "in the Cloud"

The Problem

In the past, contractors knew that their data was kept in their computer room, or perhaps on a tape stored in a backup center or a bank vault. But today, many organizations store information with a third-party storage provider out on the internet. But, in reality, all data storage is in a real location. Do you know where your data is? In some cases, this can be very important. If you have data relating to citizens of the European Union, for example, you may have responsibilities under the General Data Protection Regulation (GDPR) even though you might not be located there. In some cases, where you may be using a cloud-based service, there may be questions about whether the data is owned by you or by the service provider.

What to Do

First, all contracts for any IT related service must be reviewed by counsel. If anyone wants to use a remote service that can be paid for with a credit card, recognize that there may be terms and conditions which would be unacceptable if reviewed by counsel. Additionally, counsel should inform IT and management of any applicable laws and regulations with which the systems must comply, and where applicable, determine where data is physically stored, and any terms and conditions related to that storage. Once this is done, it may be appropriate to have the organization's compliance team check to be certain that the rules are being followed.

© 2022 Kroll. All Rights Reserved.

In this article, we've covered some of the most pressing issues in cyber and information security, but this is an area in which one size does not fit all. You may have additional issues (insiders, wireless, etc.) that need to be addressed. One idea that is important to consider is doing a written, documented risk assessment. Do you know the risks that your organization faces? How well are you dealing with those risks by mitigating them with security, transferring them through insurance or assessing some risks as being acceptable to you?

Additionally, remember that most people providing services to the construction community, whether they work for the contractor or are outsourced, may have little or no experience in responding to actual data breaches. Consider providing training that simulates attacks and teaches them how best to respond. But recognize that when a breach of your network or data is suspected or confirmed, you need to get experienced incident responders in place quickly. If you have cyber insurance, your broker or insurance carrier likely has "panels" of pre-authorized specialists in forensic investigation, breach notification, crisis communication as well as specialist counsel (sometimes called "breach coaches"). There is nothing preventing you from contacting them and pre-arranging a contract so that should an incident occur, you can engage them quickly without the potentially time-consuming contractual negotiation that might otherwise be required.

The fact is that everyone in the industry is a potential victim. With the internet, everyone lives virtually next door to cyber criminals and nation-state actors. Recognizing this is the first step in developing an effective response plan and being ready to carry it out when the time comes.

© 2022 Kroll. All Rights Reserved.

About the Author

Alan Brill
Senior Managing Director, Cyber Risk
abrill@kroll.com

Alan Brill is a Senior Managing Director with Kroll's Cyber Risk practice, based in the Secaucus office. As the founder of Kroll's global high-tech investigations practice, Alan has led engagements that range from large-scale reviews of information security and cyber incidents for multibillion-dollar corporations to criminal investigations of computer intrusions. He has worked on many of Kroll's major international projects. Alan serves as both a consulting and testifying expert in major cases where his ability to explain complex technology concepts provides counsel with a valuable litigation resource.

About Kroll

We begin this new chapter with a fresh look and a clear and confident vision for the future. United under the Kroll brand, which includes our endorsed Duff & Phelps businesses, we deliver a seamless experience across our full suite of services, with a cohesive approach to bringing tech-forward solutions to the market. Our goal is to produce greater value for our clients and partners along with compelling career opportunities for our people.

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. Built on the strength and equity of our legacy brands, we are an independent advisory firm with nearly 5,000 professionals in 30 countries and territories around the world.

Our sharp analytical skills, paired with the latest technology, allow us to give our clients clarity—not just answers—in all areas of business. For more information, visit www.kroll.com.

© 2022 Kroll. All Rights Reserved.

About Berkley Construction Professional

At Berkley Construction Professional, we transform uncertainty into opportunity so our clients can confidently build a better tomorrow. Our experienced underwriters deliver innovative, creative professional and pollution liability solutions for contractors and project owners. We respond quickly with customized coverages that fulfill the needs of our brokers and their clients. We offer practical risk management guidance and high-quality, results-oriented claims handling provided by our dedicated in-house claims professionals. Our mission is to relentlessly protect our clients' work, reputation and dreams.

Berkley Construction Professional is a division of Berkley Alliance Managers, a member company of W.R. Berkley Corporation, whose insurance company subsidiaries are rated A+ (Superior) by A.M. Best Company. berkleycp.com

For more information, contact:

Ed Sheiffele
Executive Vice President
esheiffele@berkleycp.com

Andrew D. Mendelson, FAIA
Executive Vice President,
Chief Risk Management Officer
amendelson@berkleyalliance.com

Diane P. Mika
Senior Vice President,
Risk Management Officer
dmika@berkleyalliance.com

Berkley Construction Professional
a Berkley Company

412 Mt. Kemble Avenue, Suite G50
Morristown, NJ 07960

In California:
a division of Berkley Managers Insurance Services, LLC
CA License #0H05115

Information provided by Berkley Construction Professional is for general interest and risk management purposes only and should not be construed as legal advice nor a confirmation of insurance coverage. As laws regarding the use and enforceability of the information contained herein will vary depending upon jurisdiction, the user of the information should consult with an attorney experienced in the laws and regulations of the appropriate jurisdiction for the full legal implications of the information.

Practice management recommendations should be carefully reviewed and adapted for the particular project requirements, company standards and protocols established by the construction professional.

Products and services described above are provided through various surplus lines insurance company subsidiaries of W. R. Berkley Corporation and offered through licensed surplus lines brokers. Not all products and services may be available in all jurisdictions, and the coverage provided by any insurer is subject to the actual terms and conditions of the policies issued. Surplus lines insurance carriers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

BCP Form #: PERFORM-53006-0621

© 2022 Berkley Construction Professional. All Rights Reserved.