Mitigating Top Cyber Security Risks for Architectural & Engineering Firms

The data that your firm holds on projects, people and plans has great value. Not just to your firm, but also to others who might benefit from knowing your plans, seeing your bids or stealing information about your people to carry out identity thefts.

Unfortunately, every firm, large or small, that is connected to the Internet is at risk. You may be specifically targeted because of a particular project you're working on, or you might be hit with malware looking almost randomly for sites with a particular vulnerability. The truth is that you can't achieve 100% security, particularly in an environment with growing online collaboration between organizations that may be located around the corner or around the world.

For a number of years, we've been looking at the actions taken by hackers and malware developers who have targeted firms like yours. Ultimately, you have to develop a level of security that meets three criteria:

1. It makes commercial sense for your organization. It represents a reasonable investment and does not make it unduly difficult for you and your team to do their jobs.

   Remember that only a fraction of the incidents we see are "high-tech" attacks. Most are much more straightforward, targeting a known vulnerability or involving the deliberate or thoughtless action of someone with access to your system.

2. It takes into account that despite your best efforts, you can be hit with an incident. You have to be ready and have specific plans for what to do if you think an incident has occurred.

3. Everyone in your organization takes security seriously and understands that they have a role to play in protecting your company and its information.

Specific actions to be taken will depend on the size and complexity of your company, the tools you use and with which you must collaborate, and your willingness to stress security as a business necessity. With that in mind, here are some lessons we have learned working on both preventing and responding to hundreds of incidents at businesses of all sizes and all levels of technology knowledge.

You have to do the basics, but recognize that they do not provide immunity. There are a number of fundamental steps that are so basic that they should be considered mandatory. But even with all of these in place, you can still be hit with an incident. These include:

- Know who's on your systems. This means using strong passwords that change regularly (every 90 days is common). Setting rules that require passwords to have upper and lowercase letters, at least one number and one special character is a good start.

- Make sure that anti-malware software is running on all of the devices that your people use. This isn't limited to PCs. In the world of malware developers, mobile devices are a primary target as so few people are running any kind of defensive software. It is available, and you should be using it on tablets and smartphones. Make sure that automatic updating is in place and that you maintain the subscriptions. Running out-of-date software—or not running anti-malware at all—is an invitation to disaster.

- If your people use laptop computers, you need to have full-disk encryption in place. This is now considered a best practice. It's too easy for a machine to be stolen or lost, and while the incident may be serious, if everything is encrypted, you have likely mitigated much of the potential damage. Also consider that you can encrypt portable storage devices. If you carry sensitive information on a memory stick or portable storage drive, or even on a CD or DVD, you can easily encrypt it and decrypt it when you need to use it.

Back up your data, but do it securely. Cyber-attacks are far from the only risk to your data. Hardware or software problems, mistakes by users happen every day: for example, they erase the wrong version of a file, or think they're only erasing a single file, but inadvertently destroy far more data. Knowing that you have a secure copy to use in restoring access is a business necessity. But you have to consider that the backup contains sensitive data and that it's probably going to be stored—perhaps at a storage company, perhaps online through a cloud storage provider, perhaps on a portable hard drive that you store at home—in a way that's vulnerable. For that reason, we recommend that you use encryption on your backups. You can decrypt them when you need them, but if stolen, the encryption protects your sensitive information.

Not everyone needs access to everything. You need to identify data that is sensitive and determine who actually needs access to it. While sharing and collaboration are important, the reality is that reasonable protection involves thinking about who actually needs access to various portions of your sensitive information. Limiting access reduces risk. But we've found that unless people understand why you are limiting access, they may bypass the security. For example, assume that you are busy preparing a very sensitive bid for a large project and competition for the job is fierce. You limit access to the files relating to the bid to those actually working on it. But one of those people is approached by a colleague who "wants to learn how we do bids so they can help on the next one" and asks to "borrow" the password needed to access the directory with the bid data. This might seem a very positive thing for that person to do, but what if they suddenly quit and you find them working for a firm competing for the same project? Enforcing need-to-know can be difficult, but it is a key tenet of protecting sensitive information. Need-to-know stops when someone leaves the organization. We've handled many cases where a former employee can (and does) continue to access company systems where their access is continued. Gone is gone. Even if they leave as friends, they don't need access to your networks.

You need to know what's happening in your network. Given the speed with which an incident can occur, this is vital. Part of it is knowing what your technical vulnerability is to known threats. There is software that we use that runs tests that examine every machine on your network (even things like printers, which can also have problems) and identifies any cases in which software updates ("patches") haven't been applied or where settings need to be changed to strengthen the level of protection. The other side of knowing involves keeping records or logging. You should be able to track who accessed sensitive information, know where emails came from and went to (and who sent them) and be able to identify unusual events—for example, a large encrypted file exiting your network in the middle of the night—that might signal a problem. We find too often that logs are turned off or only held for a very short time. Without logs, knowing what happened in an incident—and who was involved—can become more difficult or sometimes impossible to prove. Having good logs is an important element of your overall security program.

Consider "hardening" as a strategy. Systems often come from the manufacturer with various default settings designed to make a device easier to use. "Hardening" is the process of resetting options to provide a greater level of security. A number of organizations including the National Institute of Standards and Technology (NIST) publish hardening guides that can help with this process. However, in using these guides, you have to be careful to avoid making changes that may interfere with your particular environment. A change made to strengthen security might, for instance, render an important piece of software unable to access needed files. This is an undertaking where technical knowledge is important.

Finally, know what you will do if you believe that an incident may have occurred. The incident could directly involve your technology (for example, hacking or an employee who clicked on a phishing email and infected your network) or it might involve deliberate actions by insiders. You may need help evaluating what happened, determining what you need to do, and how and when to do it. For this reason, our final suggestion is to have a plan and have vendors identified who will be able to act quickly to help you. The skill sets you may need include (1) legal counsel with a particular expertise in data breaches; (2) forensic and investigative resources to conduct a detailed, rapid, focused inquiry and to gather and preserve vital evidence; and (3) should you have a breach involving personally identifiable information, resources to help you meet the diverse reporting requirements of 48 different state data breach statutes. Remember that each state defines what constitutes personal data. In some cases, as little as a name and home ZIP code is enough to trigger a notification requirement.

As part of your plan, you should at least consider cyber insurance. Coverage can help if you suffer a loss of sensitive data, have your systems damaged or must undertake a breach notification. Having resources identified and under contract is important because when an incident occurs, time becomes a scarce commodity. For incidents involving personal data (for example, for employees), state laws severely limit the time between discovering that there is a problem and having to carry out a notification. And a plan should be tested. You can run a simulation to make sure your people know what to do and your resources are prepared to support you as needed.

There is no magic solution to the challenge of cyber security, and clearly, each company is different, but everyone is at risk. Recognizing that risk, mitigating it to the extent reasonably possible and having a plan should the risk materialize is the only way to protect yourself. The time to start is today because your next incident could already be happening, unseen and unnoticed.

About Kroll

Kroll, the global leader in risk mitigation and response, delivers a wide range of solutions that span Investigations, due diligence, compliance, cyber security and physical security. Clients partner with Kroll for the highest-value intelligence and insight to drive the most confident decisions about protecting their companies, assets and people.

Kroll is recognized for its expertise, with 40 years of experience meeting the demands of dynamic businesses and their environments around the world. Kroll is headquartered in New York and has professionals in 45 cities across 28 countries. Learn more at krollcybersecurity.com.

About the Author

Alan Brill is a Senior Managing Director for Kroll and founder of Kroll's global high-tech investigations practice. With more than 33 years of consulting experience, Alan has assisted firms with a wide range of technology security issues. He has worked on many large-scale reviews of information security and cyber incidents and has extensive experience developing methodologies for collecting evidence from corporate information systems and consults on everything from computer intrusions to the misappropriation of intellectual property. Additionally, Alan served as an instructor for the FBI, Secret Service, Federal Law Enforcement Training Center, AICPA, and many others.