Wow! Did we screw up!

We did good. Drinks on me!

The DynaSis Education Series for C-Level Executives

Attack! How Two Companies Prepared for Ransomware

Cyber Security is no joke. If you have a business with a computer, someone is trying to hack you right now and trying to load ransomware into your system. Sooner or later, someone will get through. As common as you may think ransomware has become, studies have shown that it is even worse than you think because only a small number of victims report these attacks. **(NOTE: 5/12/17 - 150 countries hit with same ransomware attack.)** Most are embarrassed and/or afraid of negative publicity, so they just pay the ransom and move on. On top of that, Cyber criminals who used to have a tough job, now have it easy. In the old days, not only did they have to figure out how to hack into your computer, they had to actually create the malware they wanted to plant there.

Consider this: today, 91% of cyber intrusions begin through careless email practices, making it easy to gain access to your system, and the malware that he/she installs to do immeasurable harm to your system can be bought online for as little as $150. You can begin to understand that today's reality is that only constant vigilance and properly updated security measures can keep you safe.

The boy next door?

Below are two actual case studies. One details the events of a client who came on board and continually refused all our attempts to provide them with the data file and system file protection we believed they needed. The other listened to our advice and had us make the upgrades we deemed necessary to secure their files. We have changed the names of the two companies. Read what happened.

ABC Corp

In December 2015, we received a call from ABC Corp that they needed to replace their current managed IT service provider immediately. Because someone within their organization of 30-35 people had worked with DynaSis previously while at another company and trusted us, they asked for a contract ASAP. We suggested that we first provide a complimentary IT Assessment, as we do for all new clients. This is how we understand the new client's current state of security and make suggestions for adjustments so that they are adequately protected going forward.

XYZ Corp

XYZ became a DynaSis client in January of 2014. Following an IT Assessment and the usual series of on-boarding and kick-off meetings, the client agreed to certain critical infrastructure upgrades, including upgrading their on-site backup to a separate server with proper firewall protection.

Two days after ABC was hit with their ransomware attack, XYZ was hit with an attack that we believe came from the same malware kit. A few of their files were encrypted with attacks from the Netherlands and

ABC refused the IT Assessment with assurances that they would have us perform this later. They never did allow us to do so, although we asked many times.

Normal DynaSis new client procedure calls for a series of four on-boarding meetings, including an "end-user kick-off" meeting with the client's employees, during which we explain how to contact our help desk, plus an extensive training session on cyber security from the user's perspective. Company employees are often a major vulnerability and provide unwitting access to malware of all types. This kick-off training session was refused, so ABC's employees never even knew who we were nor how to contact us, nor were they trained in effective online security practices.

The "Discovery Meeting" that never happened

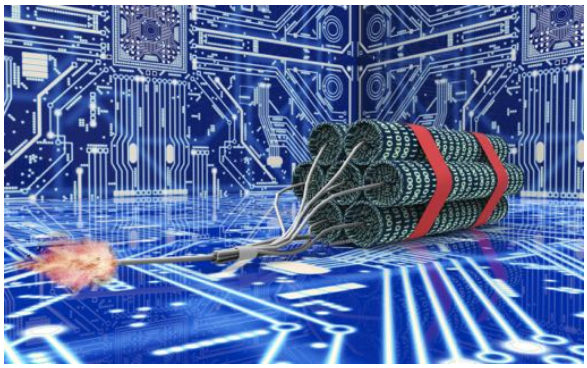
Another of the four "on-boarding" meetings we always hold is with company executives. This is our "Discovery" meeting, during which we explain how their infrastructure is setup vs. how it should be set-up. This meeting cannot take place, however, until after we have performed our IT Assessment, but as stated above, we were never allowed to do so.

DynaSis employs VCIOs (Virtual Chief Information Officers) who constantly review client status and meet with the client to make suggestions for upgrading their systems as necessary, especially at the beginning of an engagement. The VCIO assigned to ABC left phone messages, sent emails, and even stopped in and left her business card several times, but was never permitted to see the client's Executive Vice President, the person who handled IT decisions, nor did she ever receive a response. Included in these messages were warnings of the dangers that they might be facing.

Romania, but the DynaSis Crypto Containment System (CCS) immediately isolated those files, locking them out so the ransom ware virus could not spread. We were able to immediately delete the encrypted files and restore them from the backups. In less than 24 hours, they were up and running 100% with no ransom paid.

Finally, seven months after signing on as a client, the EVP agreed to meet with the DynaSis team. DynaSis sent the VCIO along with its VP of Support Delivery, who explained that there were immediate dangers that needed to be dealt with, including vulnerabilities that could allow access by cyber attackers. The ABC exec explained that they had a firewall in place, which she assumed provided protection, but the DynaSis people had previously discovered that the firewall was of consumer grade, not business grade. They also found two excellent new firewalls…but they were in their original boxes, sitting on a shelf.

It seems the previous managed IT service provider had sold ABC one of the firewalls, had been unable to install it, then sold them a second almost identical firewall, and was unable to install that. As it turned out, though, these brand new firewalls actually had insufficient capacity for the company's needs, so DynaSis provided a quote for a larger firewall and it's installation. They refused.



Disaster waiting to happen

Additionally, DynaSis people discovered that ABC's backups were being performed on the same server on which their data and system files were stored, meaning that if their primary files were attacked, their backup files might also be compromised. A very poor setup. We suggested possible upgrades: backup in-house on a separate server, or backup on an offsite server (cloud), the latter being the better option. They refused either.

More frustration ensued until one day the EVP finally admitted to the VCIO that she needed to set aside several hours of her time for an in-depth meeting and really become more involved in her company's I.T. management.

But just two days later, before this proposed meeting could even be scheduled, they were hit with a "brute force" ransomware cyber attack that encrypted all their files, **including their backups**.

Of course, they immediately called DynaSis to fix the problem, but when it was discovered that the poorly structured backups were also encrypted, it was suggested that they bite the bullet and negotiate with the hacker who had unleashed the attack, so they could at least get their system back in working order. After they negotiated the ransom down from $10,000 to $8,000, the hacker sent a test file to prove that the decryption would work…except that it didn't.

Apparently the hacker was an amateur who did not know how to use the criminal malware he had purchased and after a few attempts, he gave up, sending ABC the full but useless decryption "key" along with the note: "Good luck"…and he vanished.

Who's responsible for this disaster?

(FYI, the I.T. Assessment that DynaSis wanted to perform at the beginning of the engagement would exposed the vulnerabilities that allowed the hacker access, and the upgraded backup procedure would have prevented the encryption of the backed up files, had he somehow still gained access, although that would have been unlikely.)

When DynaSis looked at the infrastructure to try and get ABC up and running again, we found that there had been more than 65,000 failed login attempts from China, Bulgaria, Ukraine, Israel, Russia, Viet Nam, Hong Kong, the Seychelles and others. Their consumer grade firewall had worked…until it didn't.

We also discovered that the malware their hacker purchased was brand new. In fact, he apparently set it loose the same day it was released (called a "zero day" attack). This is not uncommon as new versions or strains are always being released as the bad guys attempt to keep one step ahead of us. Our analysis also told us that had they had proper on-site backup, they probably would have been okay (read about XYZ Corp's experience on the right), but cloud backup would have virtually guaranteed their security.

Two forensic decryption firms were hired to try and free up the encrypted files, but the files were deemed unsalvageable. ABC permanently lost many years of data. DynaSis has since installed proper firewall protection and onsite and off-site back to protect the client's files in the future.

Ask about our complimentary IT threat assessment.

Takeaways

- There were 65,000 attempts to access ABC's infrastructure before someone succeeded.
- Virtually every company is subject to attack every day.
- Ransoms are getting higher and higher.
- 71% of cyber attacks are now against small businesses.
- Whatever system of protection you have in place now will protect you against most attacks…until it doesn't.
- Ransomware kits are available online for as little as $150.
- These kits are often being used by amateur thieves, which makes them even more dangerous.
- Cyber insurance is available. Look into it. But understand that insurers demand that you provide top-level protection for your files.

DynaSis has been providing managed IT support and IT security to small to mid-sized businesses in the metro Atlanta area since 1992, including as a co-managed IT provider to companies with their own in-house IT teams. We belong to a nationwide network of similar IT service providers and together we research, develop and exchange the most up-to-date security solutions for our clients. It would be virtually impossible for a small to mid-sized company to attain the level of support and security we provide on their own.

For more information: www.DynaSis.com/managed-security, or call us at 678.373.0716.

DynaSis