COVENANT SECURITY SOLUTIONS INC.

ARE YOU PREPARED FOR THE NEXT RANSOMWARE ATTACK?

AT COVENANT WE HELP YOUR BUSINESS DEVELOP THE PEOPLE, PROCESS AND TECHNOLOGY SOLUTIONS TO COVER YOUR CYBERSECURITY NEEDS.

What is a Cyber Ransomware Attack?

Screenshot of WannaCry ransomware.

A week does not go by without us hearing the term ransomware. The most recent case was the "WannaCry" cyber ransomware attack, which spread globally and has caused roughly $1 billion USD in damage and is still growing. It also infected approximately 300,000 computers worldwide. As we recover from this latest version of ransomware, let's pause and understand what exactly this "ransomware" is that has all of us concerned.

"Ransomware" is malicious computer software built by a hacker that has the sole purpose of rendering your computer or device useless; unless you are willing to pay the hacker a specified amount of money, i.e. the ransom. Just like in the kidnap scene of the Hollywood blockbusters "Die Hard"; the hacker takes your computer or device hostage and requests payment(s) in order to have them either not harm your data or to release it.

The harm to your data can be done by the ransonware program encrypting it , i.e. making it unusable or not readable by you unless you have a special way to decipher the key used by the hackers to lock your data. Even more nefarious is that the ransomware can threaten to destroy or wipe out your data or to publish it publically on the internet and elsewhere unless you pay up.

Usually when this "ransonware" software is launched on your computer or device, it is done in a way so the user cannot just exit out of the "'ransomware" program. It may require the person to either pay by a set date/time or risk losing access to everything on that infected device. Loss means hackers will usually destroy /wipe out your information so that thereafter it no longer exists for your use.

The advice from the FBI and law enforcement community is mixed. Officially they encourage you **not** pay the ransom, but if you don't have measures in place to recover the lost data, then the advice is usually "just pay." If the option is lose your business and livelihood or part with a few thousand dollars or bitcoin, you will have to be the judge. The answer depends on what is appropriate in your situation. In the next section we will go into detail about the effects of ransomware such as the WannaCry virus and many others that can affect you or your organization.

Why should I care about Ransomware?

Now that we have introduced what ransomware is and the damage it can cause, do you ever wonder what a ransomware victim looks like? Too often we have images that don't always gel with reality. We often believe it is someone else that can be a victim. Just like in the photo to the left from the Disney movie "Pirates of the Caribbean"; we unknowingly assume that only unsavory characters will be victims. However, the exact opposite is true. Victims are businesses, individuals, police departments, hospitals, non-profits, i.e. anyone that can pay the ransom. The question that we hear often is "Why should I care? If the ransom is $300, maybe I can pay that and have my files back?" These questions are all valid points; however we would like to share some additional information to consider:

- Financial Cost: "Global ransomware damage costs are predicted to exceed $5 billion in 2017. Ransomware damages are up 15-fold in 2 years, and are expected to worsen. Ransomware attacks on healthcare organizations will quadruple by 2020."[1] What does this mean to you? More ransomware is coming, so paying $300 once may not be an issue for you, but with this increase it is plausible to get victimized by ransomware multiple times. However, it is more of a concern if you are a large scale organization: this $300 may be multiplied by the amount of computers and mobile devices infected, so that now a simple "let's pay" may end up being in the millions of dollars with no guarantee it will solve the problem. Secondly, it will lead to an increase in premiums for insurance, if your organization has to use a cyber policy to file a claim and maintain operations.

- Reputation: Lastly, if the files are sensitive in nature (for example protected health information (PHI), social security numbers or credit card numbers or even personal photos) the cost of an attack is high to your reputation if the files are deleted, lost or published publically. A recent survey noted; "*70 percent (of consumers) would consider leaving a retailer, 72 percent would consider leaving a financial institution, and 68 percent would consider leaving their healthcare provider, if they were hit by ransomware*."[2] This says that all customers have an expectation of privacy and protection. So as an organization, "How do I manage this risk?" We answer that next.

[1] Cybersecurity Ventures, Steve Morgan, Editor-In-Chief, 18 May 2017

[2] Carbon Black Ransomware Survey Report May 2017

What should I do to prevent a ransomware attack on my business and how should I handle my cybersecurity risks in general?

So we have covered what is ransomware and a high level view of what risk it poses to you and your organization; but what can you do to protect yourself against an attack? We understand there are many views out there, and most companies have a tool or software program. But at Covenant we recommend getting back to basics with good cybersecurity hygiene - just like you wake up every morning to wash your face, brush your teeth and comb your hair to ensure you maintain basic grooming. The same applies to preventing ransomware and lowering your risk in cybersecurity. The focus is consistency in maintaining a basic core set of functions, consistently and daily, to lower the risk of getting ransomware or any cyber risk: So what are some basic cyber hygiene items?

Risk Assessments: This step is essential to your learning where you and your organization stand early and often as it relates to people, process & technology. This means having sustained trained employee or firm support beyond just running a "scan" of your computer. A good company will support review of policies and interviews of how your company culture manages your cyber risks across your business from C-suite to the supply chain.

Patching & Backup: Do you know if your systems have the latest system updates? Do you have central control to changes of your computer and mobile software? These questions are essential - WannaCry was actually patched by Microsoft in March of 2017, so unfortunatlely many organizations suffered needlessly by not uploading the patch when initially released by Microsoft. The second key is to have a digital back up of critical data that is kept offline . Be sure to secure it and test the ability to use the back ups as well.

Awarness & Training: Do employees know what to do if they get ransomware or a virus on their computer? Invest in building a cybersecurity culture. It does not happen by running a phising test alone or once a quarter. Employees and your supply chain need training on what to look for and how to handle cyber risks. This is true both within the company and at home. Many companies have telework: so when the company data goes home, does the protection go too?

Monitoring: Cyber threats move at the speed of light. If you are a smaller organization then, at a minimum , install a firewall and virus protection. Larger organizations must have incident response plans and teams that move at the speed of light. It is still a challenge to be proactive but a key element is to have an incident response team where their process is integrated across the organization from Human Resources (HR) to Procurement. Cyber risks are not just a technical problem - rather their potential for disruption requires that all of the organization be synched to help manage this threat.

About Us

Covenant Security Solutions, Inc. is an award winning Cyber Security Company focused on providing cyber solutions that acknowledge the intersection of people, processes and technology. We provide our clients a holistic approach to meeting your Cybersecurity Risk Management needs through our CORECyber™ program.

CORECyber™ provides a subscription based managed service that covers the core of the NIST Cybersecurity Framework (CSF). For a low monthly all inclusive price we cover your Risk & Vulnerability Assessments, Compliance Management, Incident Handling & Monitoring and Cybersecurity Training & Awareness using our CATERS online platform, lastly providing certified on call support with cyber technical advisors.

Covenant provides our clients with a single interface whereby you can obtain a committed partner that can provide a holistic solution that focuses on your business needs globally and not just cyber threats.

Headquarters

Washington DC (Tysons Corner, VA)
Tel: 866-824-8022 x 800
Fax: 866-824-8022
Intl Tel: 00-1-571-201-0011

Website: www.covenantsec.com
Email: info@covenantsec.com

Additional Presence Located in: Chicago| New York| UK| India | Cote d Ivoire