HOW TO PROTECT YOURSELF FROM CYBERCRIME

Doug Marshall, Marshall Investigative Group and **Eric Rieger,** WEBIT Services

Over the past two years, I have attended several presentations regarding what to do when cyber criminals have attacked you. While these have been informative regarding the law, very little was said to protect yourself from being hacked. I wanted more information, so I consulted Eric Rieger of WEBIT Services, a friend and leading expert in the security business. I posed several questions, and he answered each in detail. He then agreed to work with me to share this information with the broader USLAW audience through this article.

Below are Eric's insights and answers to my questions about cybersecurity before an attack happens. I hope this will give you some insight into how to protect yourself and your business. We live in very unsettling times, especially with the current Russia-Ukraine War. Even though I believe we have been in cyberwar for at least the last decade, there is a visible escalation of cyberattacks on America from Russia and other threat actors. Learning steps you can take to protect, prevent and prepare are always helpful.

WHAT DO WE NEED TO DO FIRST TO ENSURE THAT OUR DATA IS SAFE?

Everything starts with a baseline risk assessment. Your risk assessment should be aligned with a recognized security framework such as NIST CSF or CIS Controls. The risk assessment results will show you where your most significant risks are, and from there, you can prioritize addressing them. This review is an ongoing, forever process, so you'll need to make it part of your company DNA to have the best chance of protecting your business.

WHAT DO YOU SEE AS THE GREATEST THREAT TO AN AMERICAN BUSINESS FROM A THREAT ACTOR?

The biggest threat we face is an attack on our utilities that would cause a mass outage, disruption to our supply chain or a mass casualty event. We came very close to seeing such an event when water treatment plants were hacked.

WHAT ARE SOME OF THE THINGS SMALL BUSINESSES CAN DO TO PROTECT THEMSELVES AGAINST CYBERCRIME?

Pick a recognized cybersecurity framework, conduct a risk assessment, set quarterly goals for remediation based on the assessment, rinse and repeat. By following a framework, you'll be following a plan that is proven to be effective and will be updated as threats change and evolve.

WHAT ARE THE MOST COMMON WAYS THREAT ACTORS COMPROMISE SENSITIVE DATA?

Business Email Compromise (BEC) continues to lead the way in entry points for threat actors. Learn more here from the FBI. Also, you're only as strong as your weakest employee when it comes to security. Employers should only give employees permissions and access to information and systems they need to successfully perform their jobs.

HOW CAN WE PROTECT OUR EMPLOYEES AND PREVENT THEM FROM MAKING CRITICAL MISTAKES?

Humans will make mistakes; it's unavoidable. The goal is to reduce the number of mistakes, create awareness and a strong security culture, and provide them with small, frequent training opportunities to test and measure their understanding. The average company will see a failure rate north of 30% the first time they conduct a phish testing campaign. With a good training program, you can typically reduce that failure rate to around 2-3% within 12 months.

WHAT ARE THE BEST PROGRAMS OUT THERE TO PREVENT ATTACKS?

The best program follows a recognized security framework like NIST and CIS Controls and is followed religiously by the organization. There are a lot of vendors out there that want to pitch their services or a piece of software, and unfortunately, they use fear-based selling instead of taking an educational approach. No single tool or process can prevent a security incident.

The goal should always be to reduce risk to a reasonable level. Following a framework will help identify risk by high probability, severe damage to low probability and low damage. If appropriately followed, any program that features education and assessments aligned with a framework should succeed.

SHOULD TWO-FACTOR AUTHENTICATION (2FA) BE PUT ON EVERY PROGRAM WITH SENSITIVE DATA, INCLUDING ACCESSING YOUR COMPUTER?

In 2019, Microsoft issued a statement saying that 99.9% of their compromised accounts did not use multi-factor authentication. Does that mean 2FA is the answer to all our security prayers? Not so much. It is an integral part of the recognized security frameworks, and any application that offers it, you should enable it for your protection. Conversely, if an application doesn't provide it, you should consider whether your organization needs that application because of its inherent risks.

2FA also comes in many flavors, of which most people aren't keenly aware. This guide from Daniel Miessler shows all the different varieties and their relative effectiveness: 2FA guide.

For additional details, visit https://www.cisecurity.org/controls/implementation-groups

HOW DO WE TEST THE SECURITY WE ALREADY HAVE?

There are many ways to test your security, and they vary in the degree of cost and effectiveness. If you follow a recognized security framework, there will be pieces along the way where testing is needed. For example, implementing a security awareness training program comes early in the process (CIS Control 14 – Group 1). But an item like penetration testing isn't recommended until the second implementation group in the CIS Controls. Penetration testing can be costly and, without a set objective, can create a false sense of security while not providing a significant return on the investment.

WHY IS SENTINEL ONE SO IMPORTANT TO SECURE YOUR DATA?

Sentinel One is part of a newer group of software protection called EDR (Endpoint Detection and Response). Traditional anti-virus software has become outdated and easily circumvented. One of the main problems with anti-virus software is it is dependent on being updated frequently, typically through a definition file it needs to download via an internet connection. Unfortunately, you're only as good as your last update in that case, and anti-virus cannot detect new "in the wild" viruses and threats we see today.

EDR solutions are typically driven by artificial intelligence and combine real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. This type of solution is far superior protection when compared with traditional anti-virus. As with any tool, it's only effective if properly deployed and monitored as part of a comprehensive security program.

CAN WE COMPLETELY STOP THE STEALING OF OUR DATA?

The short answer is no. If someone has enough time and resources (i.e., money), they can achieve the objective of stealing your information. With that being said, the goal is to make it incredibly difficult to do so, which can be an effective deterrent. Statistics show that the current average is over 200 days before a data breach is detected. That is almost SEVEN MONTHS. By implementing a proper security framework, you can significantly reduce that number over time, making you more cyber resilient and less likely to suffer a significant event.

WHAT AREAS OF THE WORLD ARE OUR GREATEST CYBER THREATS?

The usual suspects that top the list are Russia, North Korea, Iran and China. The reasoning behind the attacks varies based on origin and actor, but a great article on the recent state of security can be found in Microsoft's Digital Defense report.

HOW CAN THE U.S. GOVERNMENT HELP WITH THIS FIGHT AGAINST CYBERCRIME?

For starters, the government can create a more proactive, cohesive message. Back in 2020, the Department of Treasury issued an advisory that was not well received by the general public. In essence, the government threatened to double down on the pain suffered by U.S. businesses if they paid ransom to a cybercriminal who originated in a country currently sanctioned by the U.S. Instead of offering ways to help reduce the threat profile for U.S. businesses, the advisory is a threat without any offer of assistance.

The FBI has a history of empowering criminals when it comes to ransomware. For example, in 2015, they came out in support of paying ransoms, which I believe directly contributed to encouraging the criminals to up the ante when it came to ransom asks.

And now, more recently, the FBI told lawmakers, "it is the FBI's opinion that banning ransomware payment is not the road to go down."

To be fair, the federal government is doing more to help businesses through the CISA and Infragard, a public/private initiative aimed at informing and guiding companies to better security practices.

The best thing the government can do is invest in helping businesses adopt a recognized security framework and protect our critical infrastructure. That would go a long way towards reducing the overall risk we face as a country.

I want to thank Eric for his contributions to this article. I hope this gives readers some additional knowledge about what you may already know about protecting yourself from cybercrime.

Doug Marshall, president of Marshall Investigative Group, has been doing insurance investigative work for more than 30 years. Well known in the industry, he has been a speaker at CLM, TIDA, USLAW and the Chicago and Orlando TLA. Marshall Investigative Group's unique approach to investigations is complemented by its integrity and attention to detail.

Eric Rieger, founder and president of WEBIT Services, Inc., helps businesses evaluate the return on their technology investments, identify business risk and strategically plan technology implementations that align with the goals of the business.