Blog Posts

PRMIA 2018 Risk Management and Regulatory Compliance Round Table | Cybersecurity Aspects of Blockchain and Cryptocurrency

Welcome, my name is __. I'd like to personally thank you all for coming to my discussion on Cybersecurity Aspects of Blockchain and Cryptocurrency at the PRMIA conference in San Francisco. It is always a treat to get to talk in my hometown! For those of you unable to attend, there were two main points of topic that we went over. The first of which was about the paradigm shift in thinking about cyber security that blockchain and cryptocurrency represents. The second of which was to talk about emerging risks, and a few tips for risk managers to get started on assessing risk.

We first opened the discussion on shifting paradigms in cybersecurity, and how the metaphors we use can describe how we deploy security controls around our technology. The idea was defense in depth where there is a single asset that attackers have to overcome. The traditional defense in-depth method where the attackers are on one side of a wall, and the company assets are on the other side of the wall. All of which are protected in the middle with layers of security, control, backup control, and designed around a hard, defined perimeter. Then as the BYOD, bring your own device, and Cloud increased in popularity, the paradigm shift began. Companies started encouraging their workers to bring their own devices and use them to connect to corporate networks. The concept of the perimeter changed, adding multiple layers for users and resources. I stated that to us risk folks, the controls were similar, but the cyber criminals immediately saw the number of targets to attack increase significantly. Then the paradigm shifted to today, the new normal or as I termed it "the incredible shrinking perimeter". I talked briefly about Paypal as an example of this new normal, and how the databases are distributed outside of the company's perimeter. All while relying on new and different controls than we would see on a traditional deployment.

I then brought up the strange case of the Mt. Gox Bitcoin heist, and forgetting the fundamentals. How this cautionary tale proves that when moving quickly, one cannot forget the fundamentals. Fundamentals, such as code change and version control, segregation of duties, and prioritizing security patches. Vital things that should not be set aside in favour of moving quickly. Risk managers need to be aware of and apply these fundamentals to any risk analysis.

In closing I discussed how practices, such as an ambiguous network perimeter and distributed public databases, were once unthinkable security practices. They are now considered sound and, in many cases, superior methods to protect the confidentiality, integrity and availability of assets. Risk managers must adapt to these new paradigms and use better tools and techniques of

assessing and reporting risk. If we fail to do so, our companies will not be able to make informed strategic decisions.

Security BSides, Seattle | Can Cyber Extortion Happen to You? Practical Tools for Assessing the Threat

My name is __ and I recently had the honors of presenting at the Security BSides Conference in Seattle, Washington on Cyber Extortion and the Various Practical Tools for Assessing the Threat. I'd like to thank those of you who were able to join me for this presentation, it's always great to return to Seattle to present. For those of you who were unable to attend, there were quite a few exciting topics that were discussed. We went over how to model threats, identify assets at risk, determine the impact, and calculate risk.

We first took a look at what extortion is, down to it's legal definition and how it has extended to the cyber world. I discussed how cyber crimes have risen over the past decade to now being considered a national security threat. To the point where a task force of the FBI was designated to investigate cyber terrorists, nation state theft of IP, financially motivated crime, hacktivism and other forms of theft and sabotage. Several instances of extortion were discussed, such as the first known case of extortion of Alexander Hamilton and the 2014 SPE Hack.

We then proceeded to take a look at the three most common forms of cyber extortion – DDoS for ransom, ransomware and targeted extortion attacks. I focused in on DDoS, distributed denial of service and how in the last several years cyber criminals have picked up DDoS as an extortion tool. This type of extortion has really picked up in activity the last few years for one simples reason: it works.

The anatomy of a DDoS attack then was examined. How attackers first gather a list of websites, then launch a DDoS attack on that website list, followed by a ransom note demanding payment and threats to increase the attack if the ransom isn't paid, and lastly by either increasing the attack if the ransom isn't paid or just simply moving on. I discussed the reasons why attacks such as this work, most simply because of asymmetry. Namely cost asymmetry and information asymmetry. To illustrate this I gave the example of DD4BC, and how they utilized this type of attack to their advantage.

But then the age old question was raised, should we pay these demands? We discussed the two publicly known companies who have paid ransoms. For both instances, the only thing that stopped the attacks was purchasing DDoS protection. The bottom line from these examples was to analyze risk.

This topic was followed by looking at this from a risk-based perspective. I gave four specific tips for the detection and responses that should be taken in such instances. The first was that companies should be doing a risk analysis on your public facing websites for DDoS for ransom.

The second that once you have your risk analysis you should have two important numbers: how often this kind of attack occurs and what your annual loss exposure is.Third, to check your incident response plans and make sure you have sufficient language for these attacks. The fourth and final tip was to look at your crisis team members and make sure you have someone that has the authority to deal with ransoms in your call tree. I proceeded these tips with numerous examples of ransomware, such as the Sony Pictures hack and Ashley Madison case.

We then switched gears and talked about risk modeling. I gave the basic components of a risk assessment and how it worked with a scenario and a threat community that we'd already talked about. That the threat event frequency for a DDoS ransom attack is one of the first things you will want to you figure out. Further breaking down threat event frequency into looking at the method of the attack, the resources of the attacker, and knowing the limits of how far the threat community will go to achieve their goals. Transitioning from threat event frequency, vulnerability to these attacks was dissected, stating that vulnerability is that combination of threat capability and resistance strength. We put the threat capability of DDoS extortionists in the bottom 16%, which is not very sophisticated, but as we are only protected against the bottom 2% of attacks, this means essentially no protection. I used the Incapsula estimate to give a general risk analysis for such a loss, and utilizing residual risks I compared it what the loss would like with DDoS protection services.

In conclusion, I stressed that when an organization faces a cyber ransom, quick action is vital to responding to attackers. That these methods can help security professional understand the impact of various forms of cyber ransom, determine if it is applicable to their organization, and how to communicate risk effectively to management. This can help to strengthen incident response plans as well as the ability to make risk-aware decisions. Ransomware can and does happen to anyone - plan for it.