Journal of Information Technology Education: Discussion Cases

04/24/2017

JONATHAN ELDER, NICOLE JACOBSON, NATALIE REMSEN, KIM WILMATH

BEHIND ENEMY LINES[1]

How far should a cybersecurity company go to keep a client safe?

It was late on a Friday afternoon. The ReliaQuest Security Operations Center was busy as usual, but nothing was out of the ordinary. ReliaQuest Chief Technology Officer, Joe Partlow, was in his office working on a new technology innovation when his cell phone rang. It was the Chief Information Security Officer (CISO) for ABC Company, one of ReliaQuest's clients--a company with millions of customers across the United States. ABC Company's CISO had a crisis on his hands. He had just gotten word from his public relations staff that a journalist had called asking for a comment about a supposed leak of millions of customer records containing personally identifiable information (PTT) that could potentially be used to steal identities. Apparently, the data was listed "for sale" on the "dark web" portion of the Internet by an anonymous hacker. The CISO wanted ReliaQuest's help figuring out whether the data had, in fact, been stolen. If so, who stole it, and how? And what could be done now to re-procure the data lost? The journalist had given the company a 24-hour window before he said he would post a story.

There was also the question of whether the supposed data leak was legitimate at all. ABC Company's security team had not been able to verify that any of their systems had been breached, and there seemed to be no way to inspect the supposed stolen data without purchasing it from the anonymous hacker--something the company was not comfortable doing on its own.

The situation was urgent. The prospect of alleged customer data floating around the dark web was deeply troubling to the CISO and to Joe, yet he knew that finding the underlying cause of the situation could require members of the ReliaQuest team to use tactics outside the scope of work formally agreed upon by ReliaQuest and ABC Company. Joe also knew that if the breach was real, any tactics to identify and secure the data that ReliaQuest used could be subject to discovery in a criminal case. Moreover, Joe worried that if the breach *was* real and had somehow happened while under ReliaQuest's watch, the incident could create a public relations crisis not only for ABC Company, but also for ReliaQuest. Joe was at a high stakes crossroad for making a decision and time was of the essence. ReliaQuest prided itself on team members' willingness to do whatever it took to *make security possible* for customers. Nonetheless, Joe needed to decide: How far should ReliaQuest go to verify the breach? How would they find the underlying cause of the breach? How would they recover stolen data? And who should he consult with both within and outside of ReliaQuest to solve the problem while protecting stakeholders?

[1] Copyright © 2017, *K. Wilmath, J. Elder, N. Jacobson, and N. Remsen.* This case was prepared for the purpose of class discussion, and not to illustrate the effective or ineffective handling of an administrative situation. Names and some information have been disguised. This case is published under a Creative Commons BY-NC license. Permission is granted to copy and distribute this case for non-commercial purposes, in both printed and electronic formats. Reprinted from *Muma Case Review, 2(12)*. https://doi.org/10.28945/3928

About ReliaQuest

Joe knew that there was more at stake than just his client's customer data. For the past 10 years, ReliaQuest has grown into a national leader in IT security, serving Fortune 2000 enterprise clients around the world. ReliaQuest recognized the need for enterprise organizations to advance their security programs using tools and technologies they already owned. At that time, the only options available for security teams to address ever-changing cyber threats were to either buy more tools and technologies, or to completely outsource security to someone else. Joe and ReliaQuest CEO, Brian Murphy, saw an opportunity for what they called "co-management." Co-management provided a true security partnership that was flexible and customizable enough to evolve and advance along with new threats or security capabilities.

ReliaQuest's co-management model was built to encompass three key elements (Co-Management, n.d.):

1. Incident Response
2. Security Engineering
3. Threat Management

Security solutions were tailored to each client's specific environment, tools, risk profile and business goals, and were provided continuously--24 hours a day, 365 days a year (see Exhibit 1). Through co-management, ReliaQuest teams would work side-by-side with clients as true extensions of their teams. Client teams could advance their organization's security by leveraging ReliaQuest's security operations expertise, while ReliaQuest provided customized security solutions tailored to specific goals. This partnership put security teams in positions of support for their organization's overall business objectives, and helped them continually demonstrate returns on security investments. Cybersecurity industry experts recognized ReliaQuest's approach as the emerging industry standard for large and complex enterprise organizations. ReliaQuest's clients ranged from global Fortune 2000 organizations to regional healthcare, financial and retail organizations--with all services delivered from ReliaQuest's Security Operations Centers in Las Vegas, NV and Tampa, FL.

ReliaQuest prided itself in its commitment to doing whatever it took to keep its customers secure. More than any technique or tool, clients cited this true partnership as the key differentiator between ReliaQuest and the rest of the large and growing cybersecurity industry. ReliaQuest's customer retention rate was consistently set at nearly 100 percent.

ReliaQuest Services

As Joe pondered what to do about the alleged breach, he scanned through the three teams that made up ReliaQuest's co-management solution. Those teams consisted of Incident Response Analysts, Security Engineers and Threat Management Experts. Each team played a role in managing, monitoring and advancing client's security environments. Where along the chain might something have gone wrong in ABC Company's case? And which team members would be best suited to help find the answers he needed?

- **Incident Response:** The Incident Response teams in the ReliaQuest Security Operations Centers provided front-line defense for organizations, and were responsible for the 24/7/365 monitoring and analysis of security alerts. They investigated all alerts, filtered out false positives and escalated those alerts that required additional action or investigation to either the customer or more advanced teams within ReliaQuest. All analysts were required to undertake extensive training to ensure they were well-versed in the latest threats, tactics, techniques and procedures, and all analysts were required to complete training on the ReliaQuest Cyber Analysis

Methodology, a ReliaQuest-developed methodology for investigating cyber events. Had this team missed something during its regular screening for malicious behavior?

- **Security Engineering:** Security Engineering teams provided the next level of support to analysts and handled any technical issues that arose in customer environments. The most advanced ReliaQuest engineers had extensive industry certifications, advanced knowledge of security tools, possessed the ability to apply industry best practices, and could provide strategic recommendations to customers based on in-depth security assessments. Was something wrong with this client's suite of tools that hadn't been properly addressed by the security engineers?

- **Threat Management:** The Threat Management team was a specialized group of engineers responsible for creating all customized sets of rules and alerts to be deployed in customers' environments, which allowed analysts to better filter out anomalous or false-positive alerts. This group included the ReliaQuest Red Team--a group of ethical hackers that performed continuous testing of internal controls and analysis of external threat data to provide better security awareness (see Exhibit 2). Joe was confident that if there was something amiss, this team would be the one to help him find the root cause.

Joe had a high level of confidence in all the ReliaQuest teams. The company had always been unapologetically selective in its hiring and rigorous in its continuous training--which was vital to ReliaQuest's ability to operationalize its clients' wide variety of tools and technologies.

Joe hoped that no actual customer data had been stolen. He also hoped that would mean that no breach had occurred. But if so, why was a hacker advertising the ABC Company's data for a ransom payment. And, if there was indeed a breach of his client's customer data, how had it happened even as his own teams were co-managing security with ABC Company. He had to investigate to be sure. As a first step, Joe suspected that the Red Team, as part of the Threat Management Group, could help him the most.

Hacking the Hacker

Joe envisioned three tasks the Red Team needed to perform to obtain the information that ABC Company needed about the alleged breach. First, they would need to find a way to communicate with the seller/hacker to get a better sense of what data was available. Second, they would need to get their hands on the data itself, either via a sample from the hacker, or by actually purchasing the stolen data. Third, the team would need to carefully inspect the data, compare it to official data from ABC Company, and verify whether it was actual customers' personally identifiable information (PII) that was being sold.

This all sounded easier that it really was. When it came to communicating with the hacker, Joe and the Red Team knew they would have to use an alternate identity as to not put the ABC Company or the ReliaQuest name at risk. They would have to do so on the dark web, an anonymous sub-layer of the Internet. The dark web has been described as a "vast digital underground where hackers, gangsters, terrorists, and pedophiles come to ply their trade" (Goodman, 2015). Instead of common web browsers like Chrome or Safari or Internet Explorer, the dark web was accessed through "The Onion Router" (TOR), a U.S. Naval Research Laboratory developed network. TOR, if adroitly used, would maintain a user's anonymity, permitting clandestine communication, and enabling the purchase and sale of a cornucopia of vice and illicit goods through dark web Amazon-like shopping sites.

To limit the opportunities for surveillance and exposure, TOR was designed to route traffic to one of 6,000 volunteer relays (Skufca, 2016). The layers of encryption on the TOR network provided a layer of anonymity that was not easily breached (Exhibit 3). Though TOR was often used for nefarious means, it had also been employed by journalists, whistleblowers and even law enforcement in some cases (Exhibit 4).

Despite its usefulness, TOR was not without weaknesses. Relays had the potential to be compromised, because the nodes were run by volunteers, and exit nodes had the potential to collect data on a user's activities that could lead to identification (Osborne, 2016). Even if a user was to preserve his or her anonymity by taking the necessary security steps, there could be ways to determine a user's location, and subsequently triangulate to the user's identity (Chakravarty, Barbera, Portokalidis, Polychronakis, & Keromytis, n.d.). This could be accomplished through traffic analysis, which culled data from network routers to provide a trackable footprint that could potentially expose a user's identity.

Joe couldn't act openly as an agent of ABC Company, nor could he openly represent ReliaQuest. Joe needed to be confident in his team's ability to mask identities and shield both companies from any scrutiny that may be incurred by purchasing stolen data. Joe knew that hiding network traffic to access the data was ReliaQuest's best option. There was always a chance that the hacker selling PII on the dark web would have the sophistication necessary to dig into ReliaQuest's identity by using those advanced location pinpointing techniques. Exposure would render useless any carefully masked identity from ReliaQuest's Red Team.

Use of VPNs (Virtual Private Networks), when adroitly employed, would shield a user's location, and make it appear as if the user was located wherever the VPN originated (see Exhibit 5). When autocratic countries restricted certain websites, a VPN could circumvent that block and allow users to access forbidden information, or interact securely with other dissidents. In more typical settings, VPNs enabled users to access their company's servers remotely in a secure manner. In this case, using VPN capability would allow ReliaQuest's Threat Management Team to present themselves as a reliable buyer instead of exposing their identity as an information security company.

Joe knew this practice was unorthodox, but he also knew there was some precedent in the world of cybersecurity. Even Facebook had engaged in purchasing hacked accounts in this fashion to further strengthen their information security, paying attention to password security in vulnerable accounts (Collins, 2016).

Even with the digital trail completely masked, there were ways to inadvertently reveal a person's identity. Joe knew that hackers were notorious for being an insular group with highly specialized jargon, where any display of ignorance or terminology misused could result in a cessation of communication. To make things trickier, the jargon was constantly shifting and "for everyone hacker, there are probably a thousand suits--and suits of many different linguistic fabrics" (Crystal, 2014).

The Red Team needed to ensure that they didn't come across as corporate IT security employees. Using misspelled words and adeptly employing hacker lingo was a good first step (see Exhibit 6). Additionally, specialized hacking software helped to further obscure their syntax (see Exhibit 7). This approach helped ReliaQuest maintain anonymity to complete the purchase of the hacked data.

Now that Joe had decided how the team could access the dark web and start communicating with the hacker, he had to decide how he would go about obtaining the stolen data to investigate it. Bitcoin transactions would involve the possibility of detection, and on the dark web, this void was met by numerous unregulated cryptocurrencies. Of more than 800 cryptocurrencies that existed, Bitcoin was the most popular, with each Bitcoin valued at approximately $1,200 (see Exhibit 8). Instead of being backed by governments or gold, Bitcoin was instead based on the computational labor involved to solve complex mathematical tasks (Adamowsky, 2014). What made cryptocurrencies such as Bitcoin so popular on the dark web was that users could preserve their anonymity when making business transactions (CoinReport, 2014). The transaction details were visible, but the identities of the purchaser and seller were masked (see Exhibit 9). Because of this anonymity, there was always a risk of fraud. Once a Bitcoin transaction was complete, it was impossible to reverse.

In this case, the asking price for the stolen data was several hundred Bitcoin. But where would Joe get it? ReliaQuest did not have an existing Bitcoin account, and account limits for new users meant that Joe could not simply open a new account for that large of an amount all at once. The asking price of the hacked data was set at more than five times the daily limit for new Bitcoin users. Multiple individuals would be needed to set up sufficient funds, and to physically obtain the Bitcoin. That Friday night there was only one place to go: one of four local Bitcoin ATMs, inconspicuously located in a gas station in a neighborhood on the outskirts of town (see Exhibit 10).

Joe knew ABC Company had no choice. They needed to have the data in hand to determine the scope of the hacker's penetration into their networks. This would also reveal the severity of the attack, and help the company identify which customers might have been affected.

No Time to Waste

While Joe and the ReliaQuest Red Team worked on their plan, ABC Company's CISO continually called Joe asking for updates. ABC had trusted ReliaQuest to monitor potential security breaches for the past three years. ABC's CISO had advocated to bring ReliaQuest on as a partner which, as he explained to his own bosses, would help ABC prevent breaches like this. He needed to know whether their customer data had been stolen, and if it was, how could they mitigate this crisis as quickly as possible?

Protecting customer data was vital to ABC Company's success. The company had built itself upon the trust of its customers to provide technology solutions for communications needs. In addition to these services, ABC also offered continuous support, and boasted that its customers would have the most reliable connectivity. At the time of the alleged breach, the company had millions of customers across the country.

Because ABC held such a significant amounts of customer data, it was required to adhere to industry compliance standards via the Payment Card Industry Data Security Standard (PCIDSS). These compliance standards stipulated the precautions a company must take to ensure the safety of customer data via six goals, which included:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

A large part of the decision to partner with ReliaQuest was to meet those compliance requirements. If the customer data that was allegedly stolen was indeed PII, such as: names, addresses, social security numbers, birthdates, or maiden names, it could be used to steal customers' identities or money (PCI Security Standards Council, 2010).

While alarming, unfortunately the ABC CISO knew that this incident was not uncommon. In 93 percent of cases where data was compromised, it took attackers only minutes or less to breach the systems. But it typically took organizations weeks or more to discover that a breach had occurred.

Breaches happened in several ways. Employees with access to information could accidentally send the information to the wrong person. Insiders could misuse their privileges to information. Companies could lose important data due to loss or theft of laptops, USB drives or printed documents. Further, data could be breached from a company's system by introducing malware through an email, link, web app or website. Another common cyber-thievery mechanism was called cyber-espionage, where the thief looked for intellectual property. This technique was often used by hacking into a simple system of a given company and then using that as a stepping stone to attack other company programs.

In the case of ABC Company, which accepted credit and debit card information from its customers, there were two other ways for hackers to potentially steal personally identifiable customer data. One was point-of-sale intrusion. The company might use a database that processed transactions with customers, and this system could be compromised to steal payment information of customers. Similarly, payment card skimmers could take card information from each card that was using a payment terminal (Verizon Enterprise, n.d.).

With so many ways for companies to lose important and valuable customer data, the ABC CISO had relied on ReliaQuest for their expertise and extra security visibility at all times. Would ReliaQuest be able to provide the answers he needed before it was too late?

Prepared for Battle

Joe Partlow reviewed everything that had been running through his mind for the previous 24 hours. He had a great deal of confidence in his security analysts and engineers. His team had found no evidence of a security breach, but there was an ever-so-tiny question hovering in the back of his mind. Was it at all possible that his teams could have missed something? He had no doubt that same question was lurking around in his client's mind too. Both companies had brand reputation on the line. If ABC had in fact suffered a security breach, how would it impact the business? Would it lose customers? Would ReliaQuest's name be released to the media and then associated with the breach? How would that impact its business?

As Joe collected information and analyzed the options, the journalist that originally had given ABC Company 24 hours before releasing a story to the press, posted his story early. He then sent a follow-up email to ABC Company and provided his source from the dark web. Joe's team researched the journalist's reputation and found that this journalist had published several stories that appeared to be legitimate.

With this information and the VPN connection set up, Joe's team was ready to start communicating with the hacker on the dark web. One of his team members was ready to visit the seedy Bitcoin ATM, using a pool of funds that members of the team had pulled together from their own personal accounts. ABC Company didn't want its name anywhere near the dark web, so it would be up to ReliaQuest to act alone in purchasing the Bitcoin, working with the hacker to procure the data, and then holding their breath as they investigated whether or not the data was PII data. The question remained: Was ReliaQuest ready to pull the trigger?

The Dilemma

Joe considered his options. He knew he could reasonably let ABC Company respond to the alleged breach on its own without having his team engage in such unorthodox actions. What ABC Company needed went beyond the agreed-upon Scope of Work, which covered all the technical parameters of ReliaQuest's Threat Management Offering, but said nothing about purchasing Bitcoin and dealing directly with suspected hackers (see Exhibit 11). There were no signs that ReliaQuest was responsible for this alleged breach. By getting involved, it exposed the company to its own reputational risk. Nevertheless, if the breach was real, then ReliaQuest's brand would suffer anyway. Which was worse?

If Joe decided his team should proceed with the plan, he had even tougher decisions to make. Even though the team had hidden their identities online to reduce risk, would ReliaQuest be able to convince the seller that their identity was not a cybersecurity company or an authority? If ReliaQuest could acquire the files, how would they determine whether the data was indeed ABC customer data?

If the data was indeed from ABC, how should ReliaQuest go about a forensic investigation? Joe also knew that if the breach was real, all records of the tactics used to purchase and verify the stolen data could be subject to discovery in a criminal case.

Further, he worried that if the breach was real and had happened while under ReliaQuest's watch, the entire incident could create a public relations nightmare. As a result, he knew he would have to at some point notify other key members of the ReliaQuest leadership team, including the CEO, CFO, and others. When should he do so? And how would he explain his decision?

References

Adamowsky, E. (2014). *Bitcoin: The pros and cons for consumers and merchants.* Retrieved from https://finance.yahoo.com/news/bitcoin-pros-cons-consumers-merchants-140041526.html

Chakravarty, S., Barbera, M. V., Portokalidis, G., Polychronakis, M., & Keromytis, A. D. (n.d.). *On the effectiveness of traffic analysis against anonymity networks using flow records.* Retrieved from https://mice.cs.columbia.edu/getTechreport.php?techreportID=1545&format=pdf

Collins, K. (2016). Facebook buys black market passwords to keep your account safe. *CNet.* Retrieved from https://www.cnet.com/news/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/

Co-Management. (n.d.). Retrieved from https://www.reliaquest.com/co-management/

Crystal, D. (2014). *Language and the Internet*. Cambridge: Cambridge University Press. Retrieved from http://medicine.kaums.ac.ir/uploadedfiles/files/language_and_%20the_internet.pdf

Goodman, M. (2015). Most of the web is invisible to Google. Here's what it contains. *Popular Science.* Retrieved from http://www.popsci.com/dark-web-revealed

Osborne, C. (2016). Over 100 suspicious, snooping Tor nodes discovered. *ZDNet.* Retrieved from http://www.zdnet.com/article/over-100-spying-malicious-tor-nodes-discovered/

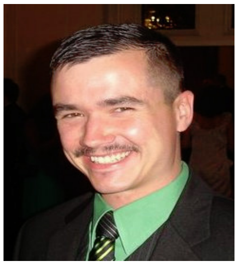
PCI Security Standards Council, LLC. (2010). *PCI DSS quick reference guide.* Retrieved from https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

Skufca, L. (2016). *The pros and cons of using Tor.* Retrieved from https://camdencivilrightsproject.com/2016/01/08/the-pros-and-cons-of-using-tor/

Verizon Enterprise, (n.d.). *Enterprise technology solutions & managed IT services.* Retrieved from http://www.verizonenterprise.com/

What are the advantages and disadvantages of Bitcoin? (2014). *CoinReport.* Retrieved from https://coinreport.net/coin-101/advantages-and-disadvantages-of-bitcoin/

Biographies



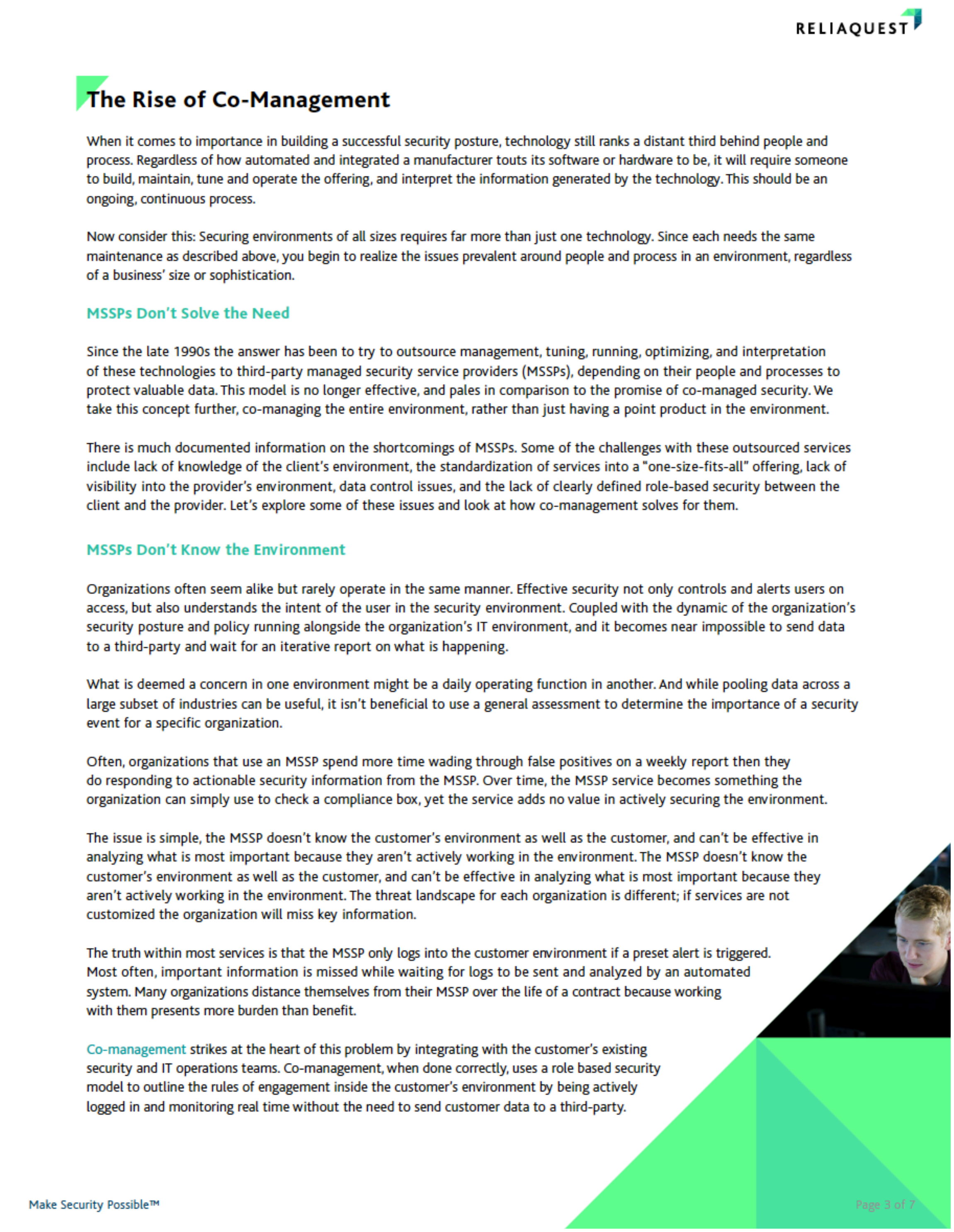
Jonathan Elder graduated from Ohio State University with a Bachelor's degree in International Relations. He has over 8 years of budget, research administration, and international training program experience, having served in the United States Navy, as well as positions within the University of South Florida, and a Veterans Health Administration Center of Innovation focusing on rehabilitation and disability research as a budget analyst. He is currently finishing his Certificate in Business Foundations.

Nicole Jacobson graduated with honors from St. Cloud State University of Minnesota with a Bachelor's degree in Communication Studies. Nicole is currently pursuing a Master's degree in Business Administration at the University of South Florida. She has over 16 years of professional work experience, with Human Resources being her focus the past 12 years. She currently serves as HR Manager, Recruiting and Administration for ArrMaz.

Natalie Remsen graduated with a Bachelor of Science degree in Microbiology from University of South Florida. She has worked at Bristol-Myers Squibb as a Clinical Trials Support Specialist since 2016. She is currently enrolled at the University of South Florida in the Master of Business Administration program.

Kim Wilmath graduated from the University of Florida with a Bachelor's degree in Journalism. She started her career as a journalist for the *Tampa Bay Times*, covering breaking news and higher education. She then transitioned into public relations, serving in communications leadership roles for the State University System's Board of Governors, for the University of South Florida, and most recently for ReliaQuest, a national leader in IT security solutions for enterprise companies around the world. She is currently pursuing her Master's in Business Administration degree at the University of South Florida.

Exhibit 1: The Rise of Co-Management



RELIAQUEST

The Rise of Co-Management

When it comes to importance in building a successful security posture, technology still ranks a distant third behind people and process. Regardless of how automated and integrated a manufacturer touts its software or hardware to be, it will require someone to build, maintain, tune and operate the offering, and interpret the information generated by the technology. This should be an ongoing, continuous process.

Now consider this: Securing environments of all sizes requires far more than just one technology. Since each needs the same maintenance as described above, you begin to realize the issues prevalent around people and process in an environment, regardless of a business' size or sophistication.

MSSPs Don't Solve the Need

Since the late 1990s the answer has been to try to outsource management, tuning, running, optimizing, and interpretation of these technologies to third-party managed security service providers (MSSPs), depending on their people and processes to protect valuable data. This model is no longer effective, and pales in comparison to the promise of co-managed security. We take this concept further, co-managing the entire environment, rather than just having a point product in the environment.

There is much documented information on the shortcomings of MSSPs. Some of the challenges with these outsourced services include lack of knowledge of the client's environment, the standardization of services into a "one-size-fits-all" offering, lack of visibility into the provider's environment, data control issues, and the lack of clearly defined role-based security between the client and the provider. Let's explore some of these issues and look at how co-management solves for them.

MSSPs Don't Know the Environment

Organizations often seem alike but rarely operate in the same manner. Effective security not only controls and alerts users on access, but also understands the intent of the user in the security environment. Coupled with the dynamic of the organization's security posture and policy running alongside the organization's IT environment, and it becomes near impossible to send data to a third-party and wait for an iterative report on what is happening.

What is deemed a concern in one environment might be a daily operating function in another. And while pooling data across a large subset of industries can be useful, it isn't beneficial to use a general assessment to determine the importance of a security event for a specific organization.

Often, organizations that use an MSSP spend more time wading through false positives on a weekly report then they do responding to actionable security information from the MSSP. Over time, the MSSP service becomes something the organization can simply use to check a compliance box, yet the service adds no value in actively securing the environment.

The issue is simple, the MSSP doesn't know the customer's environment as well as the customer, and can't be effective in analyzing what is most important because they aren't actively working in the environment. The MSSP doesn't know the customer's environment as well as the customer, and can't be effective in analyzing what is most important because they aren't actively working in the environment. The threat landscape for each organization is different; if services are not customized the organization will miss key information.

The truth within most services is that the MSSP only logs into the customer environment if a preset alert is triggered. Most often, important information is missed while waiting for logs to be sent and analyzed by an automated system. Many organizations distance themselves from their MSSP over the life of a contract because working with them presents more burden than benefit.

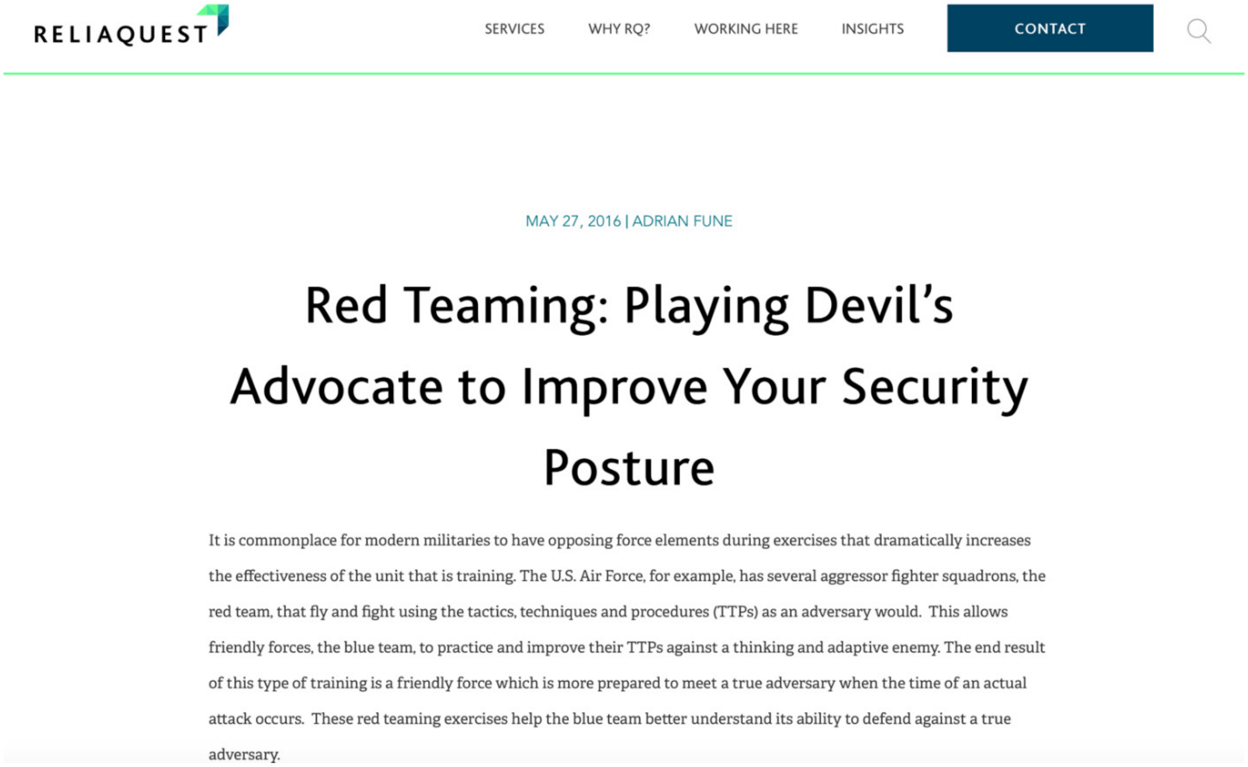
Co-management strikes at the heart of this problem by integrating with the customer's existing security and IT operations teams. Co-management, when done correctly, uses a role based security model to outline the rules of engagement inside the customer's environment by being actively logged in and monitoring real time without the need to send customer data to a third-party.

Make Security Possible™

Page 3 of 7

Source: ReliaQuest White Paper: Beyond Point Technology and The Managed Security Service Provider. Retrieved April 24, 2017, from https://www.reliaquest.com/resources/beyond-point-technology-managed-security-service-provider-mssp/

Exhibit 2: Red Teaming Exercises



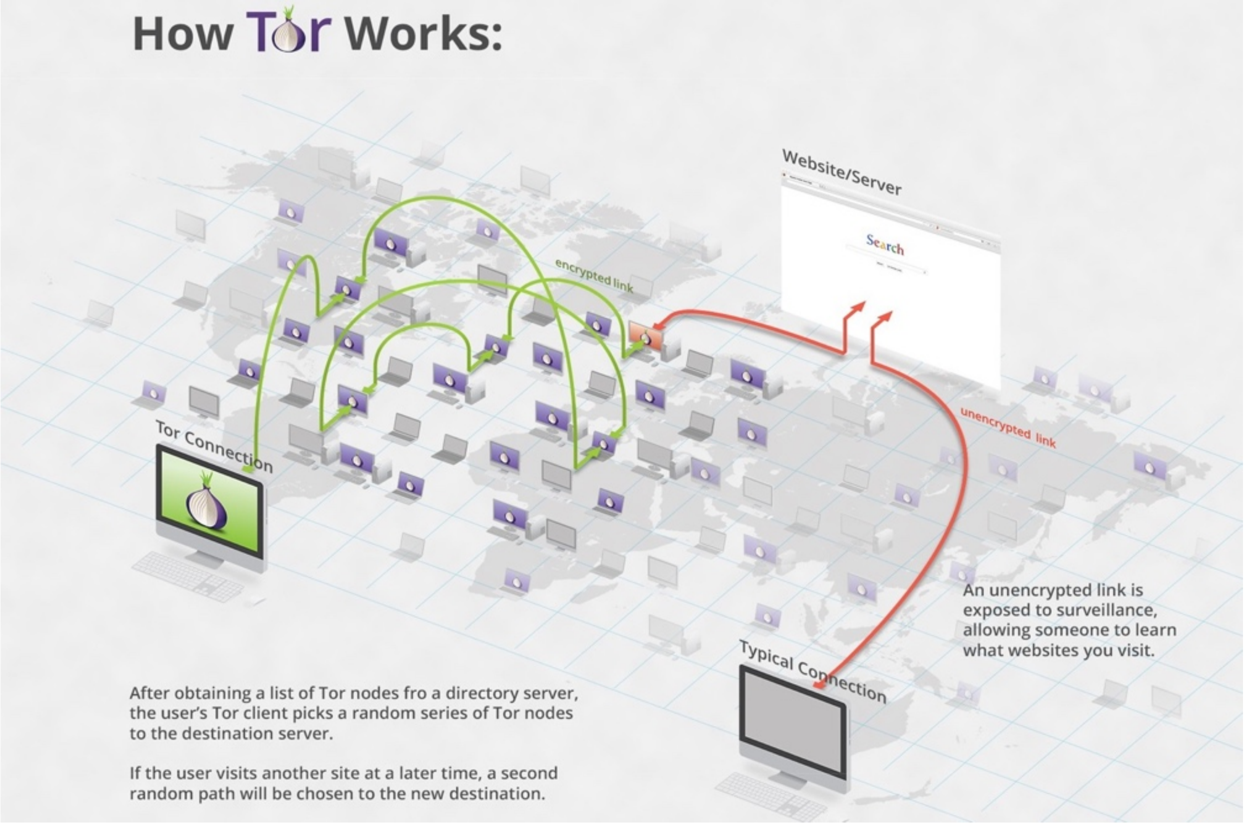
MAY 27, 2016 | ADRIAN FUNE

Red Teaming: Playing Devil's Advocate to Improve Your Security Posture

It is commonplace for modern militaries to have opposing force elements during exercises that dramatically increases the effectiveness of the unit that is training. The U.S. Air Force, for example, has several aggressor fighter squadrons, the red team, that fly and fight using the tactics, techniques and procedures (TTPs) as an adversary would. This allows friendly forces, the blue team, to practice and improve their TTPs against a thinking and adaptive enemy. The end result of this type of training is a friendly force which is more prepared to meet a true adversary when the time of an actual attack occurs. These red teaming exercises help the blue team better understand its ability to defend against a true adversary.

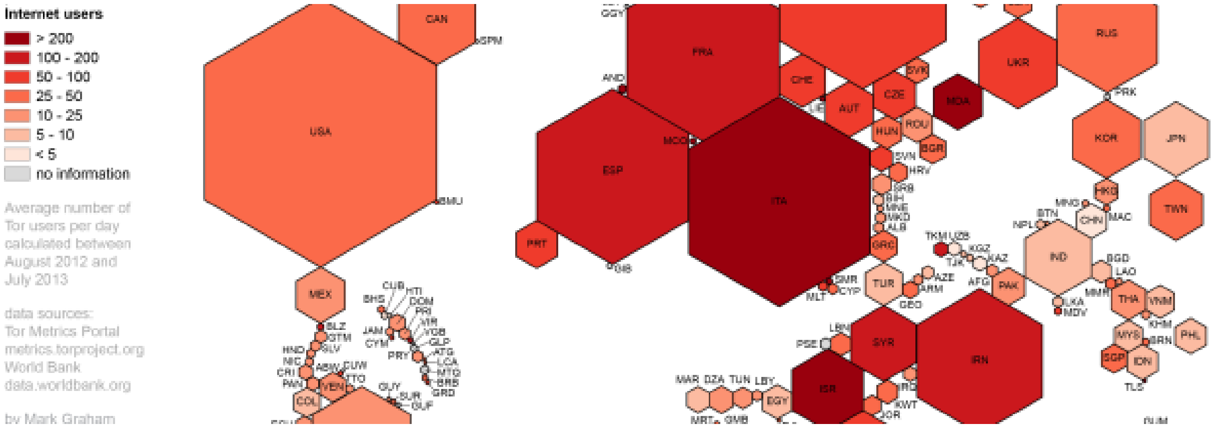
Source: ReliaQuest Blog: Red Teaming: Playing Devil's Advocate to Improve Your Security Posture. Retrieved April 24, 2017, from https://www.reliaquest.com/blog/red-teaming-playing-devils-advocate-to-improve-your-security-posture/

Exhibit 3: How TOR Works


How Tor Works:
Website/Server
Search
encrypted link
unencrypted link
Tor Connection
Typical Connection
An unencrypted link is exposed to surveillance, allowing someone to learn what websites you visit.
After obtaining a list of Tor nodes fro a directory server, the user's Tor client picks a random series of Tor nodes to the destination server.
If the user visits another site at a later time, a second random path will be chosen to the new destination.

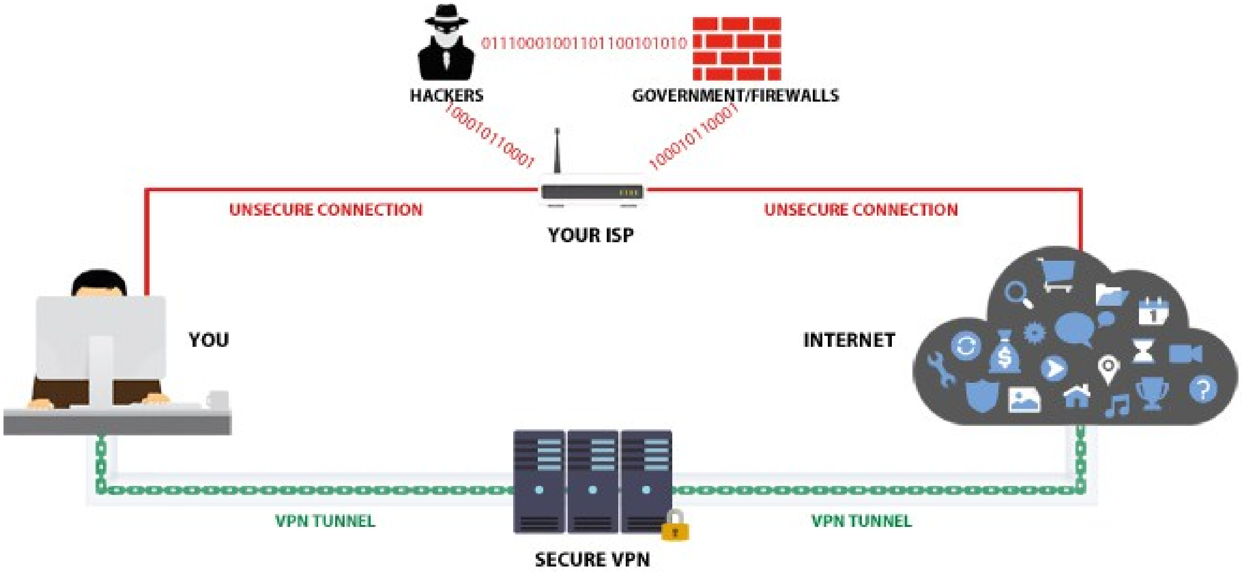
Source: How TOR Works [Digital image]. (n.d.). Retrieved April 24, 2017, from https://www.extremetech.com/wp-content/uploads/2015/12/Tor-Encryption.jpg

Exhibit 4: Geographies of TOR



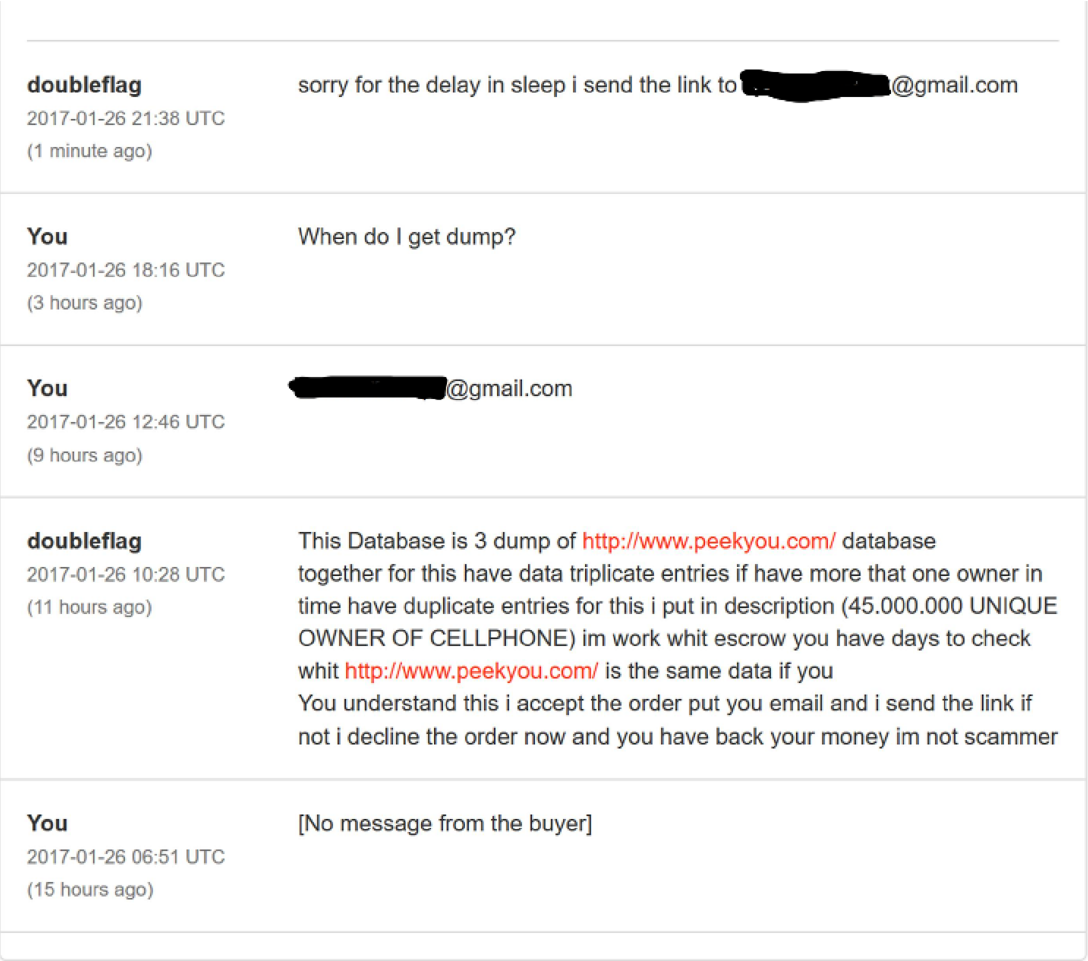
Source: Geographies of TOR [Digital image]. (n.d.). Retrieved April 24, 2017, from https://cdn.arstechnica.net/wp-content/uploads/sites/3/2015/10/Geographies_of_Tor-640x215.png

Exhibit 5: VPN Diagram



Source: VPN Diagram [Digital image]. (n.d.). Retrieved April 24, 2017, from https://i0wp.com/www.afgit.com/wp-content/uploads/2016/03/diagram.jpg?w=665

Exhibit 6: ReliaQuest Chat Logs



doubleflag
2017-01-26 21:38 UTC
(1 minute ago)

sorry for the delay in sleep i send the link to [redacted]@gmail.com

You
2017-01-26 18:16 UTC
(3 hours ago)

When do I get dump?

You
2017-01-26 12:46 UTC
(9 hours ago)

[redacted]@gmail.com

doubleflag
2017-01-26 10:28 UTC
(11 hours ago)

This Database is 3 dump of http://www.peekyou.com/ database together for this have data triplicate entries if have more that one owner in time have duplicate entries for this i put in description (45.000.000 UNIQUE OWNER OF CELLPHONE) im work whit escrow you have days to check whit http://www.peekyou.com/ is the same data if you
You understand this i accept the order put you email and i send the link if not i decline the order now and you have back your money im not scammer

You
2017-01-26 06:51 UTC
(15 hours ago)

[No message from the buyer]

Source: ReliaQuest chat logs [Screen shots]. Retrieved April 24, 2017, from ReliaQuest CTO Joe Partlow.

Exhibit 7: Syntax Encryption Examples

Charles Dickens: *A Tale of Two Cities*

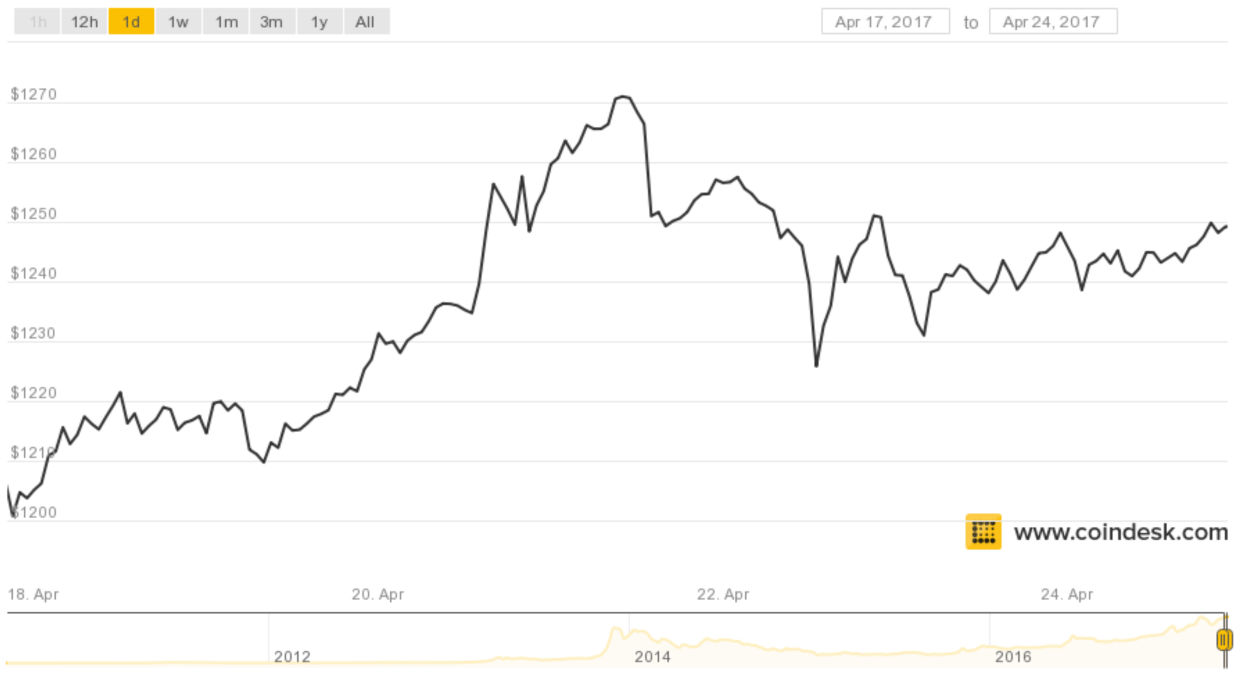
It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way – in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only. There were a king with a large jaw and a queen with a plain face, on the throne of England; there were a king with a large jaw and a queen with a fair face, on the throne of France.

Anonymous: *A Tale of Two Cities*

It was both a great time, and a poor time; the age of wisdom and of foolishness; the epoch of belief and of incredulity; the season of Light, and the season of Darkness; the spring of hope and the winter of despair; we had everything before us, we had nothing before us, we were all going direct to Heaven, and Hell. The period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, for the sake of comparison only. There were a king with a large jaw and a queen with a plain face, in England—and there were a king with a large jaw and a queen with a fair face, in France.

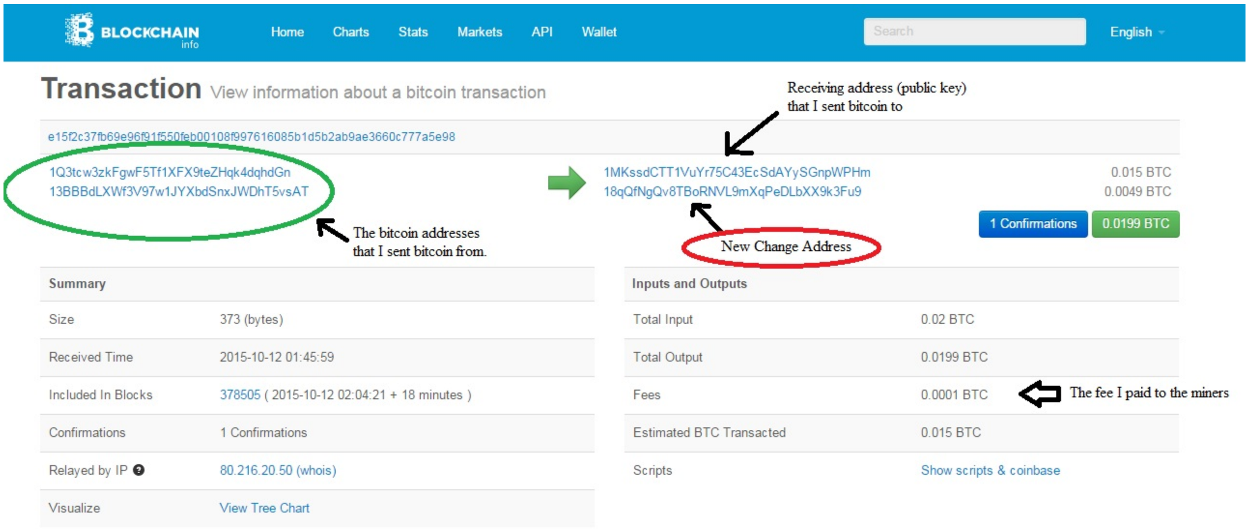
Source: Bennett, L. (2013, July 31). This Computer Program Turns Famous Writers into Anonymous Hacks. Retrieved April 23, 2017, from https://newrepublic.com/article/114112/anonymouth-linguistic-tool-might-have-helped-jk-rowling

Exhibit 8: Bitcoin Price Index Chart



Source: Bitcoin Price Index Chart [Digital image]. (n.d.). Retrieved April 24, 2017, from http://www.coindesk.com/price/

Exhibit 9: Bitcoin Transaction Details



Transaction View information about a bitcoin transaction

Receiving address (public key) that I sent bitcoin to

e15f2c37fb69e96f91f550feb00108f997616085b1d5b2ab9ae3660c777a5e98

1Q3tcw3zkFgwF5Tf1XFX9teZHqk4dqhdGn
13BBBdLXWf3V97w1JYXbdSnxJWDhT5vsAT

The bitcoin addresses that I sent bitcoin from.

1MKssdCTT1VuYr75C43EcSdAYySGnpWPHm	0.015 BTC
18qQfNgQv8TBoRNVL9mXqPeDLbXX9k3Fu9	0.0049 BTC

New Change Address

1 Confirmations 0.0199 BTC

Summary	
Size	373 (bytes)
Received Time	2015-10-12 01:45:59
Included In Blocks	378505 (2015-10-12 02:04:21 + 18 minutes)
Confirmations	1 Confirmations
Relayed by IP	80.216.20.50 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.02 BTC
Total Output	0.0199 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	0.015 BTC
Scripts	Show scripts & coinbase

The fee I paid to the miners

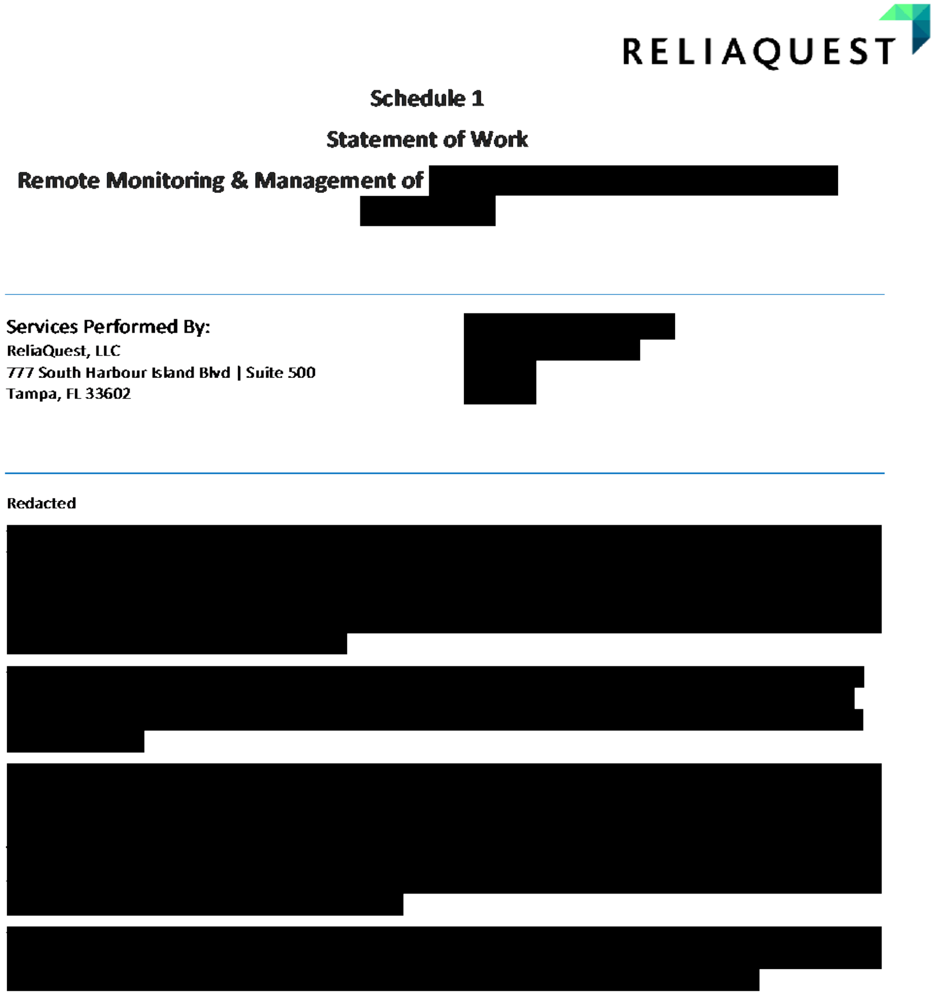
Source: Bitcoin Transaction Details [Digital image]. (n.d.). Retrieved April 21, 2017, from http://bitcoindaily.org/wp-content/uploads/2015/10/Bitcoin-Transaction-Details.jpg

Exhibit 10: Bitcoin ATM

Source: Bitcoin ATM [BitCoin ATM at Coastal Gas Station & Market]. (n.d.). Retrieved April 22, 2017, from https://coinatmradar.com/images/genesiscoin/genesiscoin_bitcoin_atm_c2ff8ff32b.jpg

Exhibit 11: ReliaQuest Statement of Work

ReliaQuest Statement of Work *(Redacted after use for case upon request by ReliaQuest)*



RELIAQUEST

Schedule 1

Statement of Work

Remote Monitoring & Management of [redacted]

Services Performed By:
ReliaQuest, LLC
777 South Harbour Island Blvd | Suite 500
Tampa, FL 33602

[redacted]

Redacted

[redacted]

[redacted]

[redacted]

[redacted]

Source: ReliaQuest Statement of Work (2017). Retrieved April 24, 2017 from ReliaQuest CFO.