

My name is Babak Pasdar, President and CEO of Bat Blue Corporation. I have given this affidavit to Thomas Devine, who has identified himself as the legal director of the Government Accountability Project, without any threats, inducements or coercion.

I have been a technologist in the computer and computer security industry for the past nineteen years and am a "Certified Ethical Hacker" (E-Commerce Consultants International Council.) I have worked with many enterprise organizations, telecommunications carriers, as well as small and medium sized organizations in consulting, designing, implementing, troubleshooting, and managing security systems. This statement is to make a record of my concerns about the privacy implications for our society from what I personally witnessed at a major telecommunications carrier, as summarized below.

In late September 2003, I received a call from a technology partner about an urgent, high-visibility project for a large wireless carrier. Our partner manufactured high performance security devices such as firewalls, and they had just won the carrier's security business.

The carrier was rolling out new picture and video technology on its phones which were forecasted to introduce increased network utilization of 50-75%. The current security tools in place were already running well over 50% of capacity, and the organization's most viable option was to go with more high performance devices.

I learned that this carrier had two disparate networks to support its mobile phone customers -- a Data network and a Cell network. We would work on the former.

The Data network supports two major areas:

Mobile Device Data Support:

The systems and tools supporting any and all data communications to the mobile device, including text messaging, Internet Communications, mobile e-mail, web access, etc.

Business Network:

The organization's business network, including systems and applications supporting sales, customer service, backups, billing, fraud detection, web applications, and systems monitoring.

The Cell network focused on the communication mechanism between the mobile devices. This included the cell towers, communications back to data centers, and connectivity of calls to land-lines or other mobile devices and providers. I did not work on this network and do not have any detailed knowledge of it.

The carrier was under immense time pressures to activate the new technologies I was brought on to implement, as it was already late September and they had a hard change freeze date in mid October. This October date was the start of what they referred to as their "Busy Season." The "Busy Season" spanned Thanksgiving through mid January, including Christmas and New Years. From my understanding, the "Busy Season" accounted for a significant portion of the organization's revenues.

The carrier's selection process had taken longer than expected, so my team came on as a technology "special forces" team to implement their new technology. The most complex aspect included conversion of over 3000 firewall policies from one firewall brand to another and implementation of the technology prior to the change freeze date. A migration on this scale had not been done before to my

knowledge, and we had to break new ground both in developing the necessary process and tools.

My team met with the client, represented by two long-term consultants (C2 and C1), who reported to the director responsible for security (DS) for the organization. C2 and C1 knew and understood the client environment and were highly competent to work well with within it. DS, however, was new to the role and came across as uncertain and tentative. He seemed concerned about making a mistake or the wrong choice in his new role. He certainly did not reference or demonstrate having any experience in the security space.

I focused on being consultative with him and made sure to spend a decent amount of time discussing both the project at hand as well as some of his other challenges with regard to his new role.

As for the project, we set out quickly to understand the client environment and to develop a game-plan for the migration.

I first focused on understanding the client's environment. C1 and C2 spent almost an entire afternoon with me touring the data center to help me understand the environment and systems impacted by our project. I realized that almost everything in the data center passed through the technologies we were brought in to work on.

We quickly pressed on to define our objectives and establish phases for the project. This included understanding the function for each of the client's firewall policies. Then it required converting the policies to a common format we could manipulate. Finally, it involved translating them from raw format to a language the new firewalls would understand.

However, we could not automate the entire effort. The two technologies had unique enough approaches to security that we had to develop a manual process for some aspects of the conversion. C2 and C1 were immensely helpful, and immediately got my team any information we needed. They were very vested in making this project a success. My calls to them in the wee hours of the morning were answered with equal immediacy as any call during the day. They became an integral part of the success we later achieved.

Once we had completed the first phase that included policy migration to the new device's format, we implemented the newly migrated policy on a pair of firewalls in the client's East Coast data center. Our plan was to test the policy set in the client environment with a select non-critical number of users. This would give us a sense of the accuracy of our conversion. It was here that we ran across our first challenge. The policy set seemed to be fine. However, the devices needed to function in a high availability mode and sustain all sessions uninterrupted through any single device outage. Unfortunately, when one device failed it seemed that the backup unit was taking over 10 seconds to establish communications and thus causing an interruption in service. This precluded high availability without impacting users, and this was just not an option. Within a short time we identified the problem and by the next day we had worked with the product manufacturer to develop a solution.

During our troubleshooting we came to realize that the client had implemented network devices called "Network VCR." They were high performance, high capacity collection devices that recorded all communications traversing any single point on the network. This allowed the client to "Record" and "Play Back" any communication between one or more systems at any point in time. On more than one occasion the client's operations team sent us communications recorded by the Network VCR from previous days to help us in the troubleshooting of a variety of issues.

While waiting for our test windows or during down-times, C1 and C2 gave me more detailed tours of the data center. They showed me the billing systems, backup system, mobile e-mail and text messaging systems, the web servers, and the log collection systems. I specifically remember being shocked at the primitiveness and inadequacy of their log collection system. After all, this was a major carrier. After a cursory overview I was able to point out to C1 and C2 that their log collection system might not have been collecting all logs. This surprised C1 and C2. A subsequent test showed that the client's log collection system was missing as many as 75% of the logs being generated, essentially rendering the whole system useless.

We received an in-depth tour of the fraud detection system from an administrator, who told us how the organization monitors all calls and narrows them to a particular set of cells, comparing any later call from a user to the original call by multiple factors, such as distance, to determine if the user would have had time to travel the distance or not. If not, it would then trigger an event with some remediation action to follow.

For example if someone makes a call from New York and then, an hour later, the same Electronic Serial Number (ESN) makes a call from Phoenix, it would be impossible to travel that distance so quickly. An alarm or event would be triggered.

Our plan that evening was to migrate a set of users to the new firewall, and then determine if and how it impacted access and functionality. We started testing and, all-in-all, the small users test migration went very well. The test went so well that we then set out to migrate over 300 sites that were carrier owned or affiliate locations. These 300 or so sites were mostly sales offices. We migrated the locations by redirecting their traffic to the new firewalls. All was going extremely well. As the night went on you could feel the relief taking over the anxiousness everyone had felt earlier.

At one point I overheard C1 and C2 talking about skipping a location. Not wanting to do a shoddy job I stopped and said "we should migrate all sites."

C1 told me this site is different.

I asked, "Who is it? Carrier owned or affiliate?"

C1 said, "This is the 'Quantico Circuit.'"

I remember that he paused and looked at me as did C2. I inquired, "Quantico, Virginia? Is this a store location?"

C1 responded, "No."

"Is it what I think it is?", I asked.

C1 did not reply but just smiled. It was a very telling smile and I knew we were discussing something unusual.

"What kind of circuit is it?", I asked.

"A DS-3," replied C1. (A DS-3 is a 45 mega bit per second circuit that supports data and voice

communications.)

C1 said that this circuit should not have any access control. He actually said it should not be firewalled.

I suggested to migrate it and implement an "Any-Any" rule. ("Any-Any" is a nickname for a completely open policy that does not enforce any restrictions.) That meant we could log any activity making a record of the source, destination and type of communication. It would have also allowed easy implementation of access controls at a future date. "Everything at the least SHOULD be logged," I emphasized.

C1 said, "I don't think that is what they want."

"Who?", I asked, and again C1 and C2 did not respond.

C2 by this point had stepped back and his body language showed that he was very uncomfortable discussing this matter.

"Come on guys, let's just do it and ask for forgiveness later. You know its the right thing." I suggested.

C1 and C2 did not want to comply. Instead they got on the phone with DS who asked me to stop what I was doing and move on. To my surprise, he then drove the one hour or so to the data center.

The tentative, uncertain DS I had known was transformed into a man wagging his finger in my face and telling me to "forget about the circuit" and "move on" with the migration, and if I couldn't do that then he would get someone who would.

I politely and in a low-key manner informed DS that my intention was to deliver security in line with industry-acceptable use scenarios, and although I am not intimately familiar with their security policy, it was reasonable to think that having a third party with completely open access to their network core was against organizational policy.

DS did not want to hear any of it and re-doubled his emphatic message to move on. This was serious stuff. He had let me know in no uncertain terms that I was treading above my pay grade.

When DS left, I asked C1 again, "Is this what I think it is?"

"What do you think?", he replied again, smiling.

I shifted the focus. "Forgetting about who it is, don't you think it is unusual for some third party to have completely open access to your systems like this? You guys are even firewalling your internal offices, and they are part of your own company!"

C1 said, "Dude, that's what they want."

I didn't bother asking who "they" were this time. "They" now had a surrogate face – DS. That told me that "they" went all the way to the top, which was why the once uncertain DS could now be so sure and emphatic.

“Does this thing have any logging or access list tied to it?”, I asked C1.

He paused, shook his head in the negative and said, “I don't think so.”

For the balance of the evening and for some time to come I thought about all the systems to which this circuit had complete and possibly unfettered access. The circuit was tied to the organization's core network. It had access to the billing system, text messaging, fraud detection, web site, and pretty much all the systems in the data center without apparent restrictions.

What really struck me was that it seemed no one was logging any of the activity across this circuit. And if they were, the logging system was so abysmal that they wouldn't capture enough information to build any type of a picture of what had transpired. Who knew what was being sent across the circuit and who was sending it? To my knowledge no historical logs of the communications traversing the “Quantico Circuit” exists.

The rest of the project went smoothly. The following week we migrated the carrier's primary location in another state successfully. Despite the success, my doubts about the purpose and legality of the “Quantico Circuit” persisted.

In interpreting what I observed, there is what I know, what is likely based on my expertise, and what is possible.

What I know:

- I know I saw a circuit that everyone called the “Quantico Circuit.”
- I know that all other sites had store numbers or affiliate numbers. The “Quantico Circuit” was the only site being migrated that had such a unique name.
- I know that it was a third party connecting to the client's network via the “Quantico Circuit.”
- I know everyone was uncomfortable talking about it.
- I know that connecting a third party to your network core with no access control is against all standard security protocols, and would fail almost any compliance standard.
- I know that I was a trusted resource. During the project, I at all times had access and control over the communications to the most sensitive of the organization's systems. This included their sales applications, billing systems, text messaging and mobile internet access, including e-mail and web. I even had a client badge for entry to the building and access to facilities.
- I know the client had Network VCRs situated at various locations throughout their data centers. These devices collected and recorded all network communications and had the capacity to store them for days, possibly weeks.
- I know that many of the organization's branch offices and affiliate systems did not have that unfettered access, because I instituted the controls.

- I know that I was withheld from implementing what the organization had deemed “standard” access control for the “Quantico Circuit.”

What is likely, based on normal industry practice:

- A third party had access to one or more systems within the organization.
- The third party could connect to one or more of the client's systems. This would include the billing system, fraud detection system, text messaging, web applications. Moreover, Internet communications between a mobile phone and other Internet systems may be accessed.
- The client could connect to one or more of the third party's systems.
- The client's Data and Cell networks are interconnected.
- It is unlikely that any logging was enabled for any access to the Quantico circuit, because the client's technical experts suggested that this was not enabled. They were tentative in even discussing the subject. Even if logging was enabled the logging system was so inappropriately sized that it was useless.

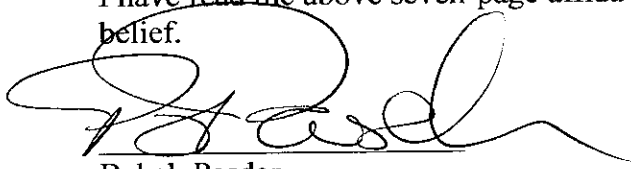
What is possible due to consistency with known facts but for which I don't have proof:

- The third party may be able to access the billing system to find information on a particular person. This information may include their billing address, phone number(s), as well as the numbers and information of other people on their plan. Other information could also include any previous numbers that the person or others on their plan called, and the outside numbers who have called the people on the plan.
- The third party may be able to identify the Electronic Security Number (ESN) of the plan member's phones. This is a unique identifier that distinguishes each mobile device on the carrier's network.
- With the ESN information and access to the fraud detection systems, a third party can locate or track any particular mobile device. The person's call patterns and location can be trended and analyzed.
- With the ESN, the third party could tap into any and all data being transmitted from any particular mobile device. This would include Internet usage, e-mails, web, file transfers, text messages and access to any remote applications.
- It also would be possible in real-time to tap into any conversation on any mobile phone supported by the carrier at any point.
- It would be possible for the third party to access the Network VCR devices and collect a variety of information en masse. The Network VCR collects all communications between two systems indiscriminately. It would then archive this information making it available for retrieval on-demand. The third party could access the Network VCR systems and collect all data

communications for single mobile device such as text messaging, Internet access, e-mail, web access, etc. over some period of minutes, hours, days or weeks. The same can be done for communications of multiple, many or even all mobile devices for some period of minutes, hours, days or weeks.

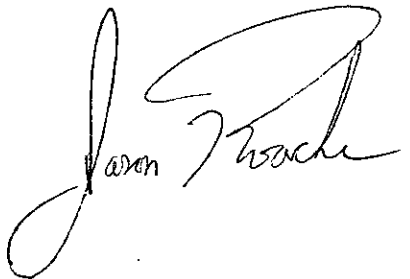
- Even if the client did not provide specific login and access for the third party to one or more of their systems, without any access controls it is possible for the third party to leverage vulnerabilities to “compromise” the client systems and obtain control or collect sensitive information.

I have read the above seven-page affidavit, and it is true and accurate to the best of my knowledge and belief.



Babak Pasdar

2/28/2008
Date



Jason Roache
Notary of New Jersey
Exp. 06/26/2012