

## The New Fluency of Risk.

### “TECHNOLOGY

accelerates congruently with risk.”

#### What is an IRL Logic Bomb?

A Logic Bomb is a piece of code intentionally inserted into software that will set off a malicious function when specified conditions are met.

An example of this was recently seen in the news. A disgruntled IT employee inserted a piece of code on over one thousand computers within his company’s network, with a detonation programmed for one month after his last login. He quit shortly thereafter, and one month later, the bomb was triggered and began rapidly deleting crucial files from computers all over the network. The code was eventually discovered and deactivated, but resulted in a \$3 million loss from the company.

IRL, is an acronym common to World of Warcraft players - who make up a population greater than the state of Ohio. IRL means, in real life, or external to cyberspace. So, an IRL Logic Bomb, is a real life manifestation of a scenario in which a factor is introduced into a system with malicious intent. To be considered a Logic Bomb, the payload should be unwanted and unknown to the user of the software.

#### In Real Life:

It’s 11a.m. on a Tuesday morning. An armored truck has just been robbed outside a local Bank of America. The suspect’s description is a man in his 20’s, outfitted in a particle mask, a dark blue shirt, jeans, safety goggles, and a yellow vest. The armored truck guard was maced by the suspect, and the suspect escaped with the cash. The only eyewitness lost sight of the man when he fled into a group of men wearing identical construction attire and matching the suspect’s physical descriptions.

How is this possible? Were all these men in identical outfits involved in the robbery? How do you find a suspect who’s description matches everyone surrounding the crime scene?

After further investigation, authorities discovered that the man had posted a job ad on Craigslist, posing as a contractor, offering \$28.50/hr to construction workers for a road maintenance project. The description in the ad instructed workers to show up on Tuesday, at 11a.m., outside

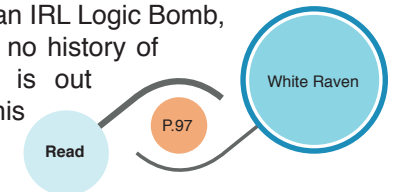
a Bank of America. As they waited for the alleged contractor, the thief, dressed as a construction worker, burglarized the armored truck, and absconded into the crowd of loitering construction workers.

Intentionally inserted data or in this case, the Craigslist instructions, which will set off a malicious function, the enabling of a robbery, makes this an IRL Logic Bomb. The payload was unwanted and unknown to the workers, law enforcement and everyone *but* the instigator.

#### If This Sounds Like Something Out of the Matrix, That’s Because it is.

Agent Smith, seen in The Matrix, is programmed to keep order within the system by terminating troublesome programs and human avatars which would otherwise bring instability to the simulated reality. Agent Smith’s persona is influenced by the popular image of federal law enforcement agents as ruthlessly efficient automata who carry out their duties with cold precision.

Agent Smith is comparable to law enforcement in its dealings with malicious code and Logic Bombs. They re-establish stability to situations through tried procedure, formed by their experience with past events, and based on what is probable. There is no set plan for stabilizing and dealing with an IRL Logic Bomb, and this is because there was no history of occurrence. What is possible is out of their realm, and that’s why this robbery was initially successful.



#### How Does This Effect Every Business?

Look at it this way. A man purchases a realistic police uniform, badge, and siren, off of eBay. He obtains a Crown Victoria from a used car lot. He drives around town pulling over innocent people who are fooled by his realistic getup, and rapes women. This happened in 2007 in Phoenix, Arizona. What is to keep individuals such as this man from infiltrating a business? A convincing law enforcement uniform and simple technological and social engineering techniques could grant him access to confidential data and sensitive materials. Some places have implemented new IDs with barcodes for all first responders. However, if the phone number for the police station can be spoofed with ease, as seen recently in Alabama, then chances are these IDs can be spoofed. This lack of security-based foresight puts everyone at risk. **When first responders cannot be trusted, who will maintain order?**

Logic Bombs are predictable on an individual basis. In the example of the armored truck burglary; increased, sensitized, surveillance would have observed the group gathering outside as suspicious activity, and could have

alerted the guards. Finding weak points in current modes of operation and technology, such as two guards instead of one, or possibly alternative methods of money transfer may mitigate the threat today. Intensive background checks for all employees; for example, could help prevent a virtual Logic Bomb. Alternative plans including data backup and emergency offsite meeting locations can help mitigate a serious breach in security. Progressive foresight and mitigation could have provided an effective plan of action.

### **Progressive Thinking is Prevention.**

Increasing complexities in the modern world mean increasing risks. The most common method of looking at risk is based on probability, which examines past events. Probability does not involve foresight, which omits any event that is possible. Looking at many recent security threats, IRL Logic Bombs in particular, businesses and individuals are ignorant to the fact that they are constantly at risk, especially because they don't have an effective mitigation plan. With technology accelerating at exponential rate, risks accelerate with it. The fact that a man can rob a bank with the help of Craigslist, and that anyone can purchase realistic law enforcement outfits, underlines the fact that with advanced technology comes advanced risks. How do we mitigate technological advances? Advanced, progressive foresight.

---

**\$28.50**

“Hourly wage offered in a Craigslist ad to roadmaintenance workers in Monroe, Washington. The dozen men who responded were used as decoys to confuse police when a thief, also dressed like a road worker, robbed an armored vehicle and fled with an undisclosed sum of money.”

---

---

### **Re:Think...**

the way we are attacked. Are we comprehending the changes in risk that technology presents? How can we battle evolving opportunities for the use of technology to destroy and damage? Are these new risks being conveyed to clients in risk assessments whether probable or simply possible?

---

## Contact

---

Kevin Burton

kevin@thinkbam.com

480.239.9724

---

Angela McGee

angela@thinkbam.com

480.239.5647