

Viewpoint Paper

**Museum Security and the Thomas Crown Affair\***

Eric C. Michaud

Vulnerability Assessment Team  
Argonne National Laboratory

Over the years, I've daydreamed about stealing a Vermeer, a Picasso, or Rembrandt. It tickles me, as much as watching the reboot of *The Thomas Crown Affair*.<sup>1</sup> Why is it, do you suppose, so much fun (despite the obvious immorality) to think about stealing a world renowned piece off the wall of a major metropolitan museum? Is it the romantic thoughts of getting away with it, walking past infrared detectors, and pressure sensors *ala* Indiana Jones with the sack of sand to remove the idol without triggering the security system? Is it the idea of snatching items with such fantastic prices, where the romance of possessing an item of such value is less intoxicating than selling it to a private collector for it to never be seen again? I suspect others share my daydreams as they watch theater or hear of a brazen daylight heist at museums around the world, or from private collections.

Though when reality sets in, the mind of the security professional kicks in. How could one do it, why would one do it, what should you do once it's done? The main issue a thief confronts when acquiring unique goods is how to process or fence them. They become very difficult to sell because they are one-of-a-kind, easy to identify, and could lead to the people involved with the theft.

The whole issue of museum security takes up an ironic twist when one considers the secretive British street artist "Banksy."<sup>2</sup> Banksy has made a name for himself by brazenly putting up interesting pieces of art in broad daylight (though many critics don't consider his work to be art) on building walls, rooftops, or even museums. I bring him up for an interesting take on what may become a trend in museum security. In March of 2005, Banksy snuck a piece of his called "Vandalized Oil Painting" into the Brooklyn Museum's Great Historical Painting Wing, plus 3 other pieces into major museums in New York. Within several days, 2 paintings had been torn down, but 2 stayed up much longer. In his

---

\* Editor's Note: This viewpoint paper was not peer reviewed.

home country of the UK, a unauthorized piece he created and placed in the British Museum known as “Early Man Goes to Market” received different treatment when placed inside the walls. It was adopted into the permanent collection! I like his story because it's so counter-intuitive. Who would have thought that modern museum security might involve preventing people not just from stealing art, but from sneaking “unauthorized” art into museums? What is next, tampering with the archive records in order to make it look like the piece in question has always been there?

To learn more about museum security, I interviewed multiple experts in the field. It turns out that the glamorous lifestyle of Thomas Crown is not particularly relevant. In fact, usually nobody can point to a Mr. Big of the underworld coordinating thefts, though some organized crime families have been known to use stolen art as black market chips to trade. The common consensus among experts in the field of art theft is that, instead of most high-value pieces being stolen by outsiders with a blue print in hand and rappelling from a ceiling skylight (exciting as this Hollywood image is), in reality, 80 percent of art thefts involve insiders or accomplices that execute the crime over a period of time while working or volunteering in the museum.<sup>3</sup> (This figure of 80% of thefts involving insiders is interesting, in that the general consensus is that in 80% of cargo thefts from trucks, the driver is involved in some manner.)

Indeed, according to FBI statistics, between 70 and 80 percent of all solved art theft cases involve insider participation of some kind, yet according to Tom Cremers of the Museum Security Network, “[Having] been involved in risk assessments in over hundreds of museums over the past ten years, it is quite astonishing how rarely the risk of insider participation is discussed.”

In regards to the insider threat, a museum is not much different from any corporation or other organization. There are directors, employees, interns, and cleaning staff (very often outsourced), security guards (again outsourced, typically with very high turnover rates<sup>4</sup>). Unlike corporations, most museums also have volunteer staff, docents, and authorized visiting scholars. All these people can potentially take advantage of their position, or to be exploited by a clever attacker on the outside or inside using social engineering.

After discussing where museum security is headed with several people involved in the field, the consensus seems to be that it is going to be completely digital at the behest of companies designing

new security products. By this I mean that nearly every security sensor and alarm is being designed so that it is compatible or adaptable to Cat 5/6 Ethernet cable. Museum security sensors are usually connected to the network infrastructure, which then gets tied back to a server monitoring the security sensors. This approach should make us feel uneasy. This is security that rides on top of technology that time and time again has proven to be highly vulnerable, and very often implemented by closed source vendors who do not release details of their code or hardware because of it being proprietary. Being proprietary is not consistent with having good security. Closed systems cannot be easily vetted by security experts for serious vulnerabilities, including stupid and easy-to-exploit ones.

What happens when the museum's security camera in the parking lot is connected via a network cable, and an attacker decides to plug his laptop onto that cable: all of a sudden he gets access to the whole network. What are the security consequences? Could this person take control of the security systems? Could he gain access to the museum's donor list (sometimes with anonymous donors) or private art appraisal values for various reasons and possibly hold the data ransom? Or just publish the information online through a site called [wikileaks.org](http://wikileaks.org) to make it public? Could tampering with computer data send a traveling exhibit to the wrong location? It seems likely that future attacks on museums may be cyber attacks, but it does not appear that museum security is being sufficiently proactive to the threat.

Another interesting question is the quality of the security provided for museum artifacts that are not currently on display, typically 85%-99% of a museum's total holdings. Are they being monitored as carefully as they should be?

Another crucial security issue for museums is that there is no international standard for reporting losses, and no public database for making the news media, art aficionados, and art dealers aware of thefts by listing missing or stolen pieces. The databases of museum thefts that do exist are disjointed and available only to a small number of museum or security professionals, who often have to pay a fee for access. If we have learned nothing from computer security and open source "Full Disclosure" policies it is that the risk of public embarrassment at being the victim of a security incident pales in comparison to doing the right thing to improve security. By publicizing what is missing or stolen, cooperative security can take place. Nothing of the sort occurs when security incidents are kept secret.

If you are interested in learning more about museum security, I have found these references to be helpful:

<http://www.museum-security.org/saz.html>

[http://en.wikipedia.org/wiki/Fence\\_\(criminal\)](http://en.wikipedia.org/wiki/Fence_(criminal))

[http://en.wikipedia.org/wiki/Elmyr\\_de\\_Hory](http://en.wikipedia.org/wiki/Elmyr_de_Hory)

<http://www.sourcesecurity.com/news/articles/co-3108-ga.3200.html>

<http://www.interpol.int/Public/WorkOfArt/Default.asp> - Interpol Art Theft Database

<http://www.fbi.gov/hq/cid/arttheft/nationalstolen.htm> – FBI Art Theft Database

*Confessions of a Master Jewel Thief*, by Bill Mason with Lee Gruendfeld (Villard, 2005), ISBN 0-375-76071-7

<http://www.artloss.com/> - Art Loss Register

<http://www.asisonline.org/councils/documents/SuggestedPracticesforMuseumSecurity.pdf> – Suggested Guidelines for Museum Security

<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html> – Passage on Vladimir Levin on the first electronic bank heist

<http://www.wikihow.com/Forge-Email>

### Acknowledgements

I am grateful to Roger Johnston for assisting with this paper.

### References

1. “The Thomas Crown Affair (1968 film),  
[http://en.wikipedia.org/wiki/The\\_Thomas\\_Crown\\_Affair\\_\(1968\\_film\)](http://en.wikipedia.org/wiki/The_Thomas_Crown_Affair_(1968_film)));  
“The Thomas Crown Affair (1999 film),  
[http://en.wikipedia.org/wiki/The\\_Thomas\\_Crown\\_Affair\\_\(1999\\_film\)](http://en.wikipedia.org/wiki/The_Thomas_Crown_Affair_(1999_film))
2. “Banksy: On Art of the State”, <http://www.artofthestate.co.uk/banksy/banksy.htm>
3. Private communication from Tom Cremers of the Musuem Security Network mailing list.
4. EG Bitzer, “Strategies for Cutting Turnover”, *Security Management* **50**(5), 88-94 (2006), based on EG Bitzer and RG Johnston, “Turnkey Turnaround Solutions: Exploiting the Powerful Tools of I/O Psychology”, Los Alamos National Laboratory Report LAUR-05-113 (2005).