FEATURED ARTICLES   FREE ENEWSLETTER   VIDEOS   ABOUT US   C

FOLLOW YOUR WAY   in   g+

TMCnet Feature
September 17, 2013

Could Better Tech Have Helped Prevent the Washington Navy Yard Shooting?

By Ed Silverstein
TMCnet Contributor

0	**1**	2	1
	Share	Tweet	Share

A 34-year-old assailant went on a shooting spree at the Washington Navy Yard this week, killing 12 people and injuring and traumatizing many others, before he was killed in an exchange of gunfire with authorities.

Even though the FBI concluded he had a valid pass to enter the complex, how could such an event happen at a military facility? Isn't there adequate technology in place to reduce the risk of such incidents?

Here's what was described in news reports. First, the shooter, Aaron Alexis of Fort Worth, Texas, had active access to enter the Navy Yard, as he worked for The Experts, a subcontractor on a Hewlett-Packard Enterprise Services contract. He was working on a project to refresh equipment used on the Navy Marine Corps Intranet (NMCI) network, HP said in a statement to Politico.

Second, for Alexis or anyone else, the way security works at the Navy complex is that employees or visitors stop at the gate. A guard checks the Common Access Card (CAC) of employees and most contractors, or the driver's license of visitors. Visitors have to report to a security office. Most cars are not searched.

Once in a building entryway, people with proper IDs can walk up to a turnstile where they swipe their CACs. A guard was stationed at the front of the entrance at Building 197 (the Naval Sea Systems Command Headquarters building), where the shooting took place. But it appears the shooter may have wounded the guard and may have even stolen his weapon. The shooter may have had up to three guns with him that day. It was reported he had an AR15, rifle and handgun. Guns are banned for civilians and all but security personnel assigned to the building. Yet there are no metal detectors at that building, sources said.

Washington Navy Yard. Image via NBC News

Because the shooter had access to the complex and likely shot his way into the building, it's hard to say how much impact technology – such as biometric access controls – would have had to limit the risk of such an incident.

"If it was an outsider, then biometric access controls can assist in preventing an individual from accessing the facility, particularly if they stole someone's identification/credentials," Jeffrey C. Price, a consultant who teaches at Metropolitan State University of Denver and is the lead security trainer for the American Association of Airport Executives, told TMCnet is an interview. "There are systems such as metal detectors and body imagers, similar to what's in use at the airports, but the question is – does the risk demand that level of response?"

Security cameras are another tool used to help out in such an attack. The Navy Yard building was equipped with many security cameras, news reports said.

"CCTV systems also help deter crime but if it's a terrorist attack of some sort, or a lone-gunman situation, then they likely will ignore CCTV anyway," Price explained. "But, CCTV can help responders to the scene to both locate the shooter and locate injured personnel."

Technology such as biometric access control devices "should be part of any access control system where the risk is high," Price added. They can scan retinas and irises, fingerprints, hands and even read veins or analyze voice prints. Each of these can identify someone through unique human characteristics.

If stolen ID cards are used, as was initially reported in the Washington Navy Yard shooting, card/PIN combinations and biometric readers would have been "effective security measures," Frank Pisciotta, president of Business Protection Specialists, told TMCnet.

In the future, there could be use of touchless screening technology to scan an individual at an airport or other facility without the person stopping, Price said. They are called the IATA (International Air Transport Association) checkpoint of the future.

There is also the more basic question if the Navy Yard should have had metal detectors in place.

"Metal detectors may provide some basic levels of protection, similar to what is used at the Smithsonian [Institution] and some of the public facilities inside Washington, D.C., and they should be deployed if the risk demands that level of response," Price said.

In the U.S. Capitol building, visitors are screened by a magnetometer. Items visitors bring into the Capitol are examined by an X-ray device.

Sometimes, rather than implementing a lot of technology and spending a lot of money on guards to

staff it, some incidents, such as the Fort Hood shooting, might have seen a better defense by improving background checks, initiating workplace violence indicator training for all personnel, or undertaking other forms of identifying signs of danger among employees, Price said.

There is also the question of training of employees and adequate planning to respond to incidents.

"Frankly, the first thoughts on identifying the potential for an active shooter and responding in the event an incident occurs is [the field of] procedures and training. Without procedures and training, there is no silver bullet in technology," Pisciotta told TMCnet.

In addition, consider how one employee told the news media "she just bolted when she's supposed to be locking down," Bo Mitchell of 911 Consulting told TMCnet.

Someone pulled a fire alarm at the Navy Yard. "This is a huge mistake. It sends personnel into the line of fire – while they are thinking 'fire,' not being fired upon," Mitchell added.

It seems clear that technology can be improved upon in a complex such as the Navy Yard. But it cannot replace adequate screening by co-workers and intelligence officials. No doubt, the security and technology at the Washington Navy Yard will be reviewed. Some policies may be changed, but the Navy Yard will never be the same.

Edited by Alisen Downey

View all articles

1 comment   ⭐ ‹ 0

Leave a message...

Best   ↪   ⚙

Bill Ofrights · a day ago
In time we'll know what surveillance cameras saw and that might shed light on what else could have been done at the time of the rampage. I think the failure happened well before that however. The Navy Yard shooter had at least two reported prior episodes when he inappropriately fired a weapon. How can a person be allowed to 1.) own guns, and 2.) be allowed into a secure workplace with that sort of backgound? Once a person establishes a pattern of dangerous behavior toward others, some actions ought to be taken to reduce the danger that person can pose to others.

     Reply   Share ›

🔊 Comment feed

✉ Subscribe via email

Related Articles

■ **Amazon Shines Up Apple Strategy with AirPlay Support**

■ **Skype Will Continue to Transform Communications Beyond 10th Anniversary**

■ **ValoreBooks Buying Used iPhones**

■ **Chromecast Support May Reach Third Parties Thanks to YouTube Testing**

■ **Apple and US Government Viewed as More Trustworthy than Twitter**

■ **Bing Refreshes Logo, Page Design**

TECHNOLOGY MARKETING CORPORATION

800 Connecticut Ave, 1st Floor East, Norwalk,
CT 06854 USA
Ph: 800-243-6002, 203-852-6800
Fx: 203-866-3326

General comments: tmc@tmcnet.com.
Comments about this site:
webmaster@tmcnet.com.

IMPORTANT

FEATURED ARTICLES
ABOUT US
VIDEOS
CONTACT US

SUBSCRIPTIONS

Subscribe to our FREE eNewsletter

Type your email here

SUBMIT

STAY CURRENT YOUR WAY