Terrifying Your Employees: Not Recommended for Training

By Michael Krausz, & M. E. Kabay, PhD, CISSP-ISSMP

The following contribution is from information security expert Michael Krausz in Vienna with editorial and textual contributions from Mich Kabay.

At a courthouse in Austria, on 28 February 2012, a security-training exercise went wrong.

In the weeks running up to the events of 28 February, police forces and the courthouse management were involved in planning what they believed to be a bright idea: conducting an exercise for courthouse staff on how to respond to someone running amok within the building.

Such an incident had happened only a couple of months before at a different courthouse in a different state in Austria, leaving two people dead (including the perpetrator) and a number of staff severely traumatized.< http://derstandard.at/1330389968074/Klagenfurt-Amoklaufuebung-am-Gericht-Mitarbeiter-unter-Schock >

Training for such an event, by itself, was therefore not a bad idea, although such events are extremely rare in Austria (this was second such incident in about 50 years).

The exercise was executed on 28 February by police forces and conducted in an extremely realistic way. Realistic indeed: it included one simulated death, apparently by a gunshot to the head. Makeup was used to simulate injuries, and several officers were placed in the building as if they were injured persons. The supposed death was staged in front of courthouse staff who were evacuating offices.

There was one catch, though: *the exercise was entirely unannounced to staff and no preparations whatsoever were taken to prepare staff for the experience.*

The effect of this omission was devastating. By the next day 40 staff members were in treatment for severe trauma and an undisclosed number had taken sick leave. We must assume that some will suffer from post-traumatic stress disorder (PTSD) in the weeks and months to come.

In a TV interview, a courthouse spokesperson justified actions by stating that the exercise was unannounced because "…[I]t is our experience that announced exercises are not taken seriously by staff."Although this assertion may be true, it does not justify exposing staff to a potentially traumatizing experience, especially given that if people cannot determine if a situation is staged or real, they must assume that it is real.

As this is being written (mid-March 2012), the latest news about the botched training exercise is that affected staff members still receive treatment and the next in line superior court to the one affected has publicly apologized for the exercise. < http://derstandard.at/1330390059483/Klagenfurt-Amokuebung-am-Gericht-Justiz-entschuldigt-sich >

For all of us planning awareness and training, it is essential to remember that surprising, frightening, embarrassing and humiliating our colleagues will not help improve security. There is no point in going through the expense of simulations and tests if we have not prepared our teams effectively and resolved everything that can be resolved before the exercises. Having unprepared staff members also means that no one is monitoring events dispassionately – or with video footage – for an effective post-training discussion of what can be improved. Exercises are supposed to contribute to continuous process improvement, not nightmares.

We finish with sound advice from noted security expert and author Rebecca Gurley Bace < http://www.infidel.net/page1/page2/ > wrote in her chapter (#46) of vulnerability assessment (VA) in the *Computer Security Handbook*, 5th Edition< http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/ >,

> Given the relatively unconstrained spirit associated with penetration testing, it is critical that the process be managed properly. Some of the requisite management considerations mirror those of the more generic process of [vulnerability assessment (VA)]. Independent oversight is required for the conduct of VA; it is especially critical to the success of penetration testing. Test scenarios should be documented and approved in advance by at least two representatives of the organization being tested, and the employees of the organization should be prepared for testing, especially when social engineering techniques are included in the scope of penetration testing.
>
> This set of agreements and preparation for testing is key to balancing the need to perform realistic and relevant VA (including penetration testing) with the need to minimize the impact of such testing on normal business operations.
>
> As human systems and constructs are as much a part of business operations as information systems, minimizing impact involves consideration of the ethics of social engineering. The first ethical tenet asserts that social engineering tests should not cause psychological distress to test subjects. Most employees are conscientious with regard to security and other company policies and may consider being targeted by social engineering tests as a breach of trust. Their reactions to that perceived breach may range from anger to resignation, or to a lawsuit.
>
> Another ethical tenet states that those who fail social engineering or other penetration tests should not be subject to humiliation; this requires that test results be treated as confidential information. Finally, testers should not rely unduly on verbal misrepresentation or acting to achieve the goals of testing—the objective of such testing is to establish whether security measures are appropriate and effective for the organization, not to score a win for the test team at all costs. To leave a tested organization in worse condition than the test team found it is a hollow victory for all involved.

So forget dreams of Hollywood special effects and a compelling theatre experience: involve employees in all preparations for exercises, drills, simulations and tests.

* * *

Michael Krausz studied physics, computer science and law in university. He is a professional investigator as well as lead auditor for ISO27001 compliance. He designed the first ever information security training classes in Austria (1998) and has assisted in setting up certifying bodies and accreditation authorities for ISO27001/ISO27006. Having worked in 14 countries so far on a range of information security topics, Mr. Krausz has published two English-language books on managing information security breaches [*Information Security Breaches: Avoidance and Treatment Based on ISO27001* < http://www.amazon.com/Information-Security-Breaches-Avoidance-Treatment/dp/1849280274/ > & *Managing Information Security Breaches* < http://www.amazon.com/Managing-Information-Security-Breaches-

Michael/dp/1849280940/ >]. He has recently published a German-language book on the dangers and challenges the Internet for the individual and the state in collaboration with the head of the Cybercrime Unit at the Austrian Federal Criminal Intelligence Agency, Mr. Leo Löschl [*Schauplatz Cyberworld*, < http://www.amazon.de/Schauplatz-Cyberworld-Leopold-L%C3%B6schl/dp/3902494557/ref=sr_1_1?ie=UTF8&qid=1332099651&sr=8-1>]. Mr. Krausz is a national member of ISO’s JTC1/SC27/WG1 committee and editor of ASIS’s investigation council’s newsletter.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *