Physical Threats to the Information Infrastructure (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this occasional series, I am showcasing some of the best short essays submitted by students in information assurance and cybercrime courses and programs at Norwich University. John Orlando, PhD, is the Administrative Director of the MSIA (Master of Science in Information Assurance) program at Norwich; in compliance with the policy instituted by Dean Fred Snow, he is participating in the MSIA program as a student. He submitted this work as one of his weekly essays in November. The rest of this column and the next is a slightly edited version of his report on physical security at Norwich University. I hope that readers will be able to apply his findings to their own institutions as an example of what to look for in securing facilities.

* * *

When one thinks of threats to an information infrastructure, one tends to conjure up images of electronic assaults, such as virus and denial-of-service attacks. But the greatest threats to an electronic infrastructure come from more mundane sources. Water, fire, or theft cause far more damage than electronic attack, but we think about them less because physical disasters receive far less media publicity than the more exotic electronic assault.

In this essay I examine the protections against physical threats to Norwich University’s information infrastructure. I will divide the threats into two categories, natural and man-made, and will examine each in turn. Not all threats are equally likely, or equally harmful and thus my analysis will include a consideration of the relative risks of each threat, the potential harm involved, and the protections currently in place against the risk. As usual, I will end with some recommendations.

Natural Threats

In terms of potential damage, floods certainly present a serious danger to an information infrastructure. Water short circuits operating computer systems, and damages hardware. Owing to its mountainous geography, Vermont faces a greater threat of flood than many other regions, but Norwich University sits atop a hill high above the nearest water source, the Rock River. It would take a flood of biblical proportions for water levels to reach the IT unit. A more likely scenario finds high water taking out telephone and power lines. As mentioned in a prior section, there are power and telephone backups in place to handle such a scenario.

Wildfires can also have a catastrophic impact on computer systems if they severely damage the building in which such systems are housed. Though Norwich University is in a forested region, Vermont’s type of foliage, along with its less than dry climate, make wildfires far less of a threat than in other regions. It’s been quite a while since Vermont has witnessed a serious forest fire. Moreover, Norwich University it fairly well insulated from the surrounding forest by large fields, and thus the threat of wildfire is quite low. As with floods, fires present a greater danger to the power and phone lines that feed Norwich University’s IT systems than the systems themselves.
In areas of strong seismic activity, earthquakes can present a considerable threat to IT systems. Unlike wildfires and floods, where the building in which the IT system is housed protects that system, it is precisely the surrounding structure that presents a threat with earthquakes. Earthquakes in Vermont are rare, but not unheard of. As recently as June, 2002, a 4.9 earthquake rocked the Champlain Valley, causing some minor damage. However, it would take a much stronger earthquake to threaten the fairly sturdy building in which Norwich University’s IT system sits, one of a magnitude which has probably never been recorded in the state.

Temperature presents another threat to information systems. Computer performance tends to deteriorate above certain temperatures, and high humidity can cause corrosion to circuits and other hardware. While Vermont is not known for its oppressive heat, temperatures can rise to the 90s with high humidity on occasion, just enough to place certain sensitive computer systems in jeopardy. In response to the danger, the computer room at Norwich University is climate controlled with three compressors, each of which can mediate the temperature and humidity in the room by itself. Thus, there is considerable redundancy in the HVAC system. Even if the HVAC system did fail, the IT department can simply shut down its computer systems to reduce harm to the components.

* * *

In the next article, Dr Orlando looks at man-made threats to the physical infrastructure.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 John Orlando. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.