Velocihackers and Tyrannosaurus superior

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Information Assurance & Statistics
School of Business & Management
Norwich University, Northfield VT

In the early 1990s, I used to write for the paper version of Network World. Recently I was watching the 1993 hit movie "Jurassic Park"< http://www.imdb.com/title/tt0107290/ > and I recalled a column I wrote back then that cause a flurry of comment and that may interest current readers. Here's a slightly updated version of that old column.

* * *

"Jurassic Park" stars several holdovers from 65 million years ago. It also shows errors in network security that seem to be as old.

For those of you who are too young to have seen it, "Jurassic Park" is about a dinosaur theme park that displays live dinosaurs created after scientists cracked extinct dinosaur DNA code recovered from petrified mosquitoes. The film has terrific live action dinosaur replicas and some heart stopping scenes. It also dramatizes awful network management and security. Unfortunately, the policies are as realistic as the dinosaurs.

Consider a network security risk analysis for Jurassic Park. The entire complex depends on computer controlled electric fences and gates to keep a range of prehistoric critters from eating the tourists and staff. So at a simple level, if the network fails, people turn into dinosaur food.

Jurassic Park's security network is controlled by an ultramodern Unix system, but its management structures date from the Stone Age. There is only one person who maintains the programs which control the security network. This breaks Kabay's Law of Redundancy, which states, "No knowledge shall be the property of only one member of the team." After all, if that solitary guru were to leave, go on vacation, or get eaten by a dinosaur, you'd be left without a safety net.

Jurassic Park's security system is controlled by computer programs consisting of two million lines of proprietary code. These critical programs are not properly documented. An undocumented system is by definition a time bomb. In the movie, this bomb is triggered by a vindictive programmer who is angry because he feels overworked and underpaid.

One of the key principles of security is that people are the most important component of any security system. Disgruntled and dishonest employees cause far more damage to networks and computer systems than hackers. The authoritarian owner of the Park dismisses the programmer's arguments and complaints as if owning a bunch of dinosaurs gives him the privilege of treating his employees rudely. He pays no attention to explicit indications of discontent, including aggressive language, resentful retorts, and sullen expressions. If the owner had taken the time to listen to his employee's grievances and take steps to address them, he could have prevented several dinosaur meals.

Bad housekeeping is another sign of trouble. The console where the disgruntled programmer works looks like a garbage dump; it's covered in coffee cup fungus gardens, historically significant chocolate bar wrappers, and a treasure trove of recyclable soft drink cans. You'd

think that a reasonable manager would be alarmed simply by the number of empty calories per hour being consumed by this critically important programmer. The poor fellow is so overweight that his life expectancy would be short even if he didn't become dinosaur fodder.

Ironically, the owner repeats, `No expense spared' at several points during the movie. It doesn't seem to occur to him that with hundreds of millions of dollars spent on hardware and software--not to mention the buildings and grounds and an entire private island--modest raises for the staff would be trivial in terms of operating expenses but significant for morale.

In the movie, the network programmer is bribed by competitors to steal dinosaur embryos. He does so by setting off a logic bomb that disrupts network operations completely. The network outage causes surveillance and containment systems to fail, stranding visitors in, well, uncomfortable situations. Even though the plot is not exactly brilliant, I'd like to leave at least something to surprise those who haven't seen the movie yet.

When the systems fail, for some reason all the electric locks in the park's laboratory are instantly switched to the open position. Why aren't they automatically locked instead? Normally, when a security controller fails, the default should be to keep security high, not eliminate it completely. Manual overrides such as crash bars (the horizontal bars that open latches on emergency exits) can provide emergency egress without compromising security.

As all of this is happening, a tropical storm is bearing down on the island. The contingency plan appears to consist of sending almost everyone away to the mainland, leaving a pitifully inadequate skeleton crew. The film suggests that the skeleton crew is not in physical danger from the storm, so why send essential personnel away? Contingency plans are supposed to include redundancy at every level. Reducing the staff when more are needed is incomprehensible.

At one point, the systems are rebooted by turning the power off to the entire island on which the park is located. This is equivalent to turning the power off in your city because you had an application failure on your PC. Talk about overkill: why couldn't they just power off the computers themselves?

Where were the DPMRP (Dinosaur Prevention, Mitigation and Recovery Planning) consultants when the park was being designed? Surely everybody should know by now that the only way to be ready for dinosaurs, uh, disasters, is to think, plan, rehearse, refine and update. Didn't anyone think about what would happen if the critters got loose? Where are the failsafe systems? The uninterruptible power supplies? The backup power generators? Sounds like Stupidosaurians were in charge.

We may be far from cloning dinosaurs, but we are uncomfortably close to managing security with all the grace of a Brontosaurus trying to type.

I hope you see the film. And bring your boss.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at

Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >