Can Nature Help Us Solve Risk Management Issues?

Position Paper

William H. Saito

William@saitohome.com

Abstract. As a member of the commission that investigated the Fukushima (Japan) nuclear disaster and studying other catastrophes over the past century, it was discovered that all were man made and preventable; all resulted from a lack of understanding of risk and/or a refusal to accept numerous warnings and risk assessments. The lessons of Fukushima show clearly that true security planning is not a quest for absolutes (100 percent reliability), but a flexible response to the inevitability of system failures. One of the best approaches to understanding and modeling IT security is to begin with a deep understanding of biological processes in Nature. Because many contemporary security problems have analogues in the natural world, effective solutions to these problems may already exist. By ignoring them we are trying to reinvent the wheel.

Keywords: Nature, Risk, Resilience, Evolution, Biology, Systems, Fukushima

A long time ago, towards the end of the 20th century, the software company that I founded in California developed its own suite of security applications and solutions, so it was only natural for us to study all the commercially available security tools on the market. Soon we were digging deeper into the science behind authentication, encryption and more. As our business grew, we developed a set of biometric interface standards that Microsoft ultimately adopted as part of the Windows operating system. Along this journey my interest in and knowledge about information security deepened, and I found myself advising both public- and private-sector organizations. But it was only a few years ago that I sat down and began writing about encryption, authentication, digital signatures and fairly technical aspects of cryptography as well as other esoteric aspects of security.

Then came 3.11. No, not 9.11, but March 11, 2011, the day a massive earthquake and tsunami ripped across the northeastern coast of Japan. It was only then that the life-and-death importance of risk management and its profound implications for all types of security became apparent. Terrible as the natural devastation was, the tsunami precipitated an even more terrifying event, leading to the near-destruction of the Fukushima Dai-ichi Nuclear Power Plant.

Later that year, I was appointed the Chief Technology Officer for the Fukushima Nuclear Accident Independent Investigation Commission[1], an ad hoc body reporting to the national legislature (it was, in fact, the first independent investigation ever commissioned by the National Diet of Japan). That position provided a unique opportunity to examine this catastrophe in detail and to see its multiple causes. Looking at the long chain of errors and misjudgments that led up to Fukushima naturally brought my thinking around to the idea of security and risk management. How could the risks not have been more widely foreseen? How could the management of that risk have been so inept? What steps were taken after the accident to limit risk and what steps were put in place subsequently to prevent a similar situation from occurring?

One of my tasks as CTO was to develop a secure IT system that would allow the members of the new Commission to share and store information, ideas, notes and comments freely and flexibly without the danger of outsiders gaining access to those private discussions. How could over a hundred participants from various regions of Japan, and with widely varying levels of computing proficiency, securely conduct a sensitive investigation without accidentally or intentionally leaking information by, say, losing a personal computer or being subject to a hacker attack? Thankfully, because the IT system was designed from the ground up with security planning as a primary directive, the Commission was able to conduct its work over a period of months and publish its findings without any information being manipulated, destroyed or leaked.

When the post-3.11 world finally began to settle down, my perspective had changed and I now viewed the whole field of IT security through the broader lens of risk management. I had never liked talking about security from a purely technical perspective, which by definition misses the big picture, and after 3.11 my feelings grew even stronger. My experiences studying the Fukushima disaster and managing security for the Commission further reinforced my belief that "doing IT security" simply by designing sophisticated new authentication systems or cryptography algorithms was not the right approach. It misses the critical component of risk management. As the old adage says, security is only as strong as the weakest link in the chain. Real security, and not only in the world of IT, lies in maximizing your field of view, expanding your thinking, for example, by canvassing the natural world for useful examples, and even expanding your imagination to encompass what has never yet existed.

The catalyst for my change in perspective began a month before the start of the commission. Not being a nuclear safety or risk management expert, I took it upon myself to study all the historically significant disasters. Thus, I spent most of my yearend holiday reading over 4,000 pages of reports on disasters as varied as the Titanic, Challenger, Three Mile Island, Chernobyl, Concord, BP, Katrina and many others. What I realized was that all these catastrophes had one major factor in common: they were all preventable. That is, in each case the relevant engineers saw the

[1] for more information about the disaster, its causes and consequences, see The National Diet of Japan – Fukushima Nuclear Accident Investigation Commission (NAIIC) home page: http://naiic.go.jp/

potential for problems and warned their superiors, but in each case senior managers dismissed those warnings, often due to a kind of hubris I call the "It can't happen here" syndrome. More importantly, they did not comprehend the risks.

The Fukushima disaster was no different; in fact, it was totally preventable. Warnings had been issued for years, warnings that would have been red flags to any risk management officer, but those warnings were ignored. The Commission said as much in their conclusion: "What must be admitted — very painfully — is that this was a disaster 'Made in Japan'... Its fundamental causes are to be found in the ingrained conventions of Japanese culture: our reflexive obedience; our reluctance to question authority; our devotion to 'sticking with the program'; our groupism; and our insularity."[2] They might also have echoed Dr. Richard Feynman, who concluded his addendum to the official report on the Challenger disaster with these famous words: "For a successful technology, reality must take precedence over public relations, for nature cannot be fooled."[3]

In the end, to do any kind of security, we must take to heart the a priori precepts of risk management: a) people make mistakes, b) machines eventually break and c) accidents inevitably happen. True risk management is not a quest for absolutes (100% fail-proof operation over the life of a system), but a practice in resilience, in predicating one's thinking on the assumption that *all systems will sooner or later fail in some way*. If that is your starting assumption, then real "security" becomes a challenge in how best to *recover* from all types of accidents, break-downs and system failures, both foreseeable and as yet unimagined.

We Are All Risk Management Creatures

The most important thing to understand about "security" and risk management in general is that these are not new additions to human thinking, but an intrinsic part of our oldest, most basic brain structures. In fact, the most fundamental security systems are "built in" – they're literally part of our DNA. Nor are we unique in this aspect; Nature has risk management in its genes. Which means we don't "learn" security-type thinking — we adapt, develop and (occasionally) improve on aspects of our natural heritage. This is what Einstein was getting at when he said, "Look deep into Nature, and then you will understand everything better."

We are all risk management creatures. When we wake up in the morning, without even thinking about it, we smell the air and listen for certain sounds. If we're at home and there's no perceived threat, we will naturally be less attentive to our surroundings than if we awoke, say, in an unfamiliar hotel room. Yet even in the comfortable, "risk-free" environment of our own homes, we're still safety-checking constantly, from instinctively scanning the stairs for objects that don't belong there to smelling

[2] http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/wp-content/uploads/2012/09/NAIIC_report_lo_res10.pdf

[3] Feynman, R.P., "Personal observations on the reliability of the Shuttle"; Report of the Presidential Commission on the Space Shuttle Challenger Accident, Appendix F (1986)

the milk before it goes in our coffee. Getting in the shower, getting dressed, sipping that hot coffee, eating breakfast, watching the weather report — by the time we go out the door in the morning we have done a hundred routine risk management checks. Most of them require little or no conscious attention. We'd say they're habits, but that's not entirely correct; they've become habits precisely because the fundamental templates were biologically coded. We do these things instinctively because we are security-oriented, risk-management animals to begin with. All larger, more sophisticated approaches to controlling risk are variations on or amplifications of Nature's basic instincts of self-preservation. Humans, like all biological creatures, cannot eliminate risk; but by instinctively performing many small risk-mitigating actions, we usually manage to avoid the more serious negative outcomes, like dying.

First, Look to Nature

It is this background that causes me to take a step back when I hear discussions of the newest security technologies. "Why re-invent the wheel?" I say. "If you're faced with a security problem, you should start by looking at how similar problems are dealt with in Nature." I'm not sure why this attitude seems so radical, because to me it seems pretty obvious. Before you start to tell me about the newest, coolest, "unbreakable" code, first show me that you've thought about, or at least that you're aware of analogous situations in the natural world.

Here's a simple, elegant example: think about how a human egg is fertilized. One and only one sperm is allowed to get inside that egg, and once it does, the vault doors are closed and locked. This *non-repudiation* "system" prevents polyspermia through electrical or chemical means while authenticating the spermatozoa itself[4]. I argue that such examples should be our starting point when we talk about, e.g., financial systems that need to specify and authenticate one and only one transaction.

Look at how white blood cells (lymphocytes), penicillin and other antibiotics *authenticate* and attack certain bacteria but leave others untouched. Or how DNA replication includes a regular checkpoint mechanism[5] that verifies the *integrity* of the copying process, thus ensuring that replication occurs perfectly every time. Our immune system has spent millions of years evolving into a decentralized and distributed control system that consists of billions of cells working together to manage a huge variety of threats in a robust, scalable and flexible manner. *Resilience* manifests itself in many ways, including organisms that switch between sexual and asexual reproduction depending on environmental conditions. The mechanism for cell signaling comprises at least six different communication methods, including hormones that transmodulate and *encode* different signals for different pathways.

---

[4] Gilbert SF. Developmental Biology. 6th edition. Sunderland (MA): Sinauer Associates; 2000. Gamete Fusion and the Prevention of Polyspermy.

[5] Noguchi, E. The DNA Replication Checkpoint and Preserving Genomic Integrity During DNA Synthesis; 2010 Nature Education 3(9):46

In a truly "eat or be eaten" world, viral, bacterial and animal species have developed both offensive and defensive mechanisms to protect themselves, including cloaking, stigmergy and mimcry, which clearly have IT security analogues, such as polymorphic, APT, botnet, DDoS, phishing and pharming attacks. While the security industry discovers and responds to a seemingly endless profusion of threats, our bodies and Nature in general have been constantly fighting a far greater war just to stay alive.

Not Short-term Solutions, but Sustainable Success

There are thousands of other examples of efficient, effective security solutions, both "out there" in the natural world and within our own bodies. Today's IT systems are still at a fairly primitive stage of mimicking existing natural systems. Natural systems work exceedingly well because of a single key difference between their design and modern, man-made systems — their risk control "protocols" are an integral part of their being. Their security "code" is written in DNA; it's designed-in from the start, not added on later as an afterthought.

The other overwhelming characteristic of the natural world, and the one that has produced so many risk management responses in animals and plants, is the process of evolution. Remember that basic fact: Nature *evolves* — it changes; it learns; it gets better – it is resilient. Yes, a whole species may suffer, and in extreme cases it might nearly die out, but the "system" learns. It responds, it discovers ways to neutralize threats, and eventually it triumphs over those threats. That "flexible response" is another key to long-term, sustainable success. It is interesting to note that the same tradeoffs in terms of cost, speed, and security vs. convenience that concern us in modern system design can also be studied in the natural world. The latter systems have evolved over hundreds of millennia to provide the optimum mix of security and efficiency.

Our security needs will continue to increase as fast as new technologies are commercialized to make our lives faster and easier. Ironically, we will need to fundamentally rethink our approach to security in order to remain up to date in this changing environment. The problem will always be: How do we keep ourselves and our data safe in an increasingly interconnected world? The answers may be closer than we think, based on hints we discover in the natural world.