Help Wanted: Cyber Security Neurologist

Jack Hampton is a Professor of Business at St. Peter’s University in New Jersey and a former Executive Director of the Risk and Insurance Management Society (RIMS). He was named a Risk Innovator in 2008 by Risk and Insurance®. His website is www.jackhampton.com.

When we think about how some companies protect their electronic assets, it brings to mind “leech therapy.” This method has been used since ancient times to treat illness and disease. Many cyber security efforts resemble it. We perform a procedure and the patient improves. We don’t know if it was our treatment or just luck. We take credit for the success either way.

Medical advancement recognized that the human body is constantly under attack by unseen aggressors. At a basic level, antibiotics kill bacteria. We prevent heart attacks by reducing cholesterol and high blood pressure. Surgeons eliminate cancer by exorcising tumors.

At more complex levels, doctors move past a single remedy. Pharmaceutical cocktails treat HIV, and cancer and holistic medicine helps us understand the need to make lifestyle changes.

These lessons are needed in cyber risk management. Information technology specialists build firewalls and insist upon complex passwords. They work at one level but fall short in the face of constantly mutating electronic pathogens.

To start, we need agreement on cyber security goals. The risk manager seeks to avoid damage to assets, interruption to operations and liability lawsuits. The underwriter wants to identify and insure named perils and avoid all-risk policies that cannot identify black
swans. The CFO wants insurance to protect big losses but balks at incurring high costs without assurance that massive cyber damage will be reimbursed by the coverage. These individual viewpoints can be reconciled by a “cyber security neurologist,” an individual with the knowledge and training to protect the total cyber body.

A neurological disorder is an abnormality in the brain, spinal cord or nervous system. Damage includes paralysis, seizures, confusion and pain. A cyber neurological disorder can affect the (1) “brain” (computers, servers, and knowledge of work force), (2) electronic “central nervous system” (business disruption and liability) and (3) “peripheral nervous system” (liability exposures with customers, suppliers, partners and regulators).

There are many medical neurological disorders, some relatively common, but many quite rare. They may be treated by different specialists using preventative measures, lifestyle changes, physiotherapy, pain management and surgery.

Cyber neurological disorders are often treated differently. Organizations build firewalls without changing practices, processes and cultural lifestyles that leave doorways open. If this is your perspective, the next step is likely to be pain management.

What if we treat cyber risk like a peanut disorder, a type of hypersensitivity provoked by an allergen? A medical study just turned treatment on its head. Previously, doctors diagnosed the allergy and told us to keep totally away from any food with even a trace of peanut content. Teenage and adult peanut intolerance soared with this guidance.

A new study shows allergen immunotherapy or desensitization dramatically increases tolerance. Small doses of peanut butter starting with infants greatly reduces the likelihood of the disorder later on.

Cyber immunotherapy could treat the whole system. We can sensitize authorized users and correct behaviors that are careless or unmindful. We can separate data that needs the highest security from routine information available all over the internet. We can recognize that cyber risk is not a disease that needs an IT brain surgeon when the real problem is we are not protecting the entire electronic neurological system.

In conclusion, you may ask, “Why does everyone pick on poor leech therapy?” To comply with the Equal Time Rule, you are directed to Mehdi, a self-described Leech Therapist in Australia. He points out bloodletting “is still thriving today.”

Sony Pictures, Yahoo and the Democratic National Committee are victims of recent cyber attacks. Maybe they needed more than electronic “bloodletting.”

End of article
Risk Insiders are an unrivaled group of leading executives focused on the topic of Risk. They share their insights and opinions – and from time to time their pet peeves and gripes.

Risk Insiders are invited to publish based on their expertise, passion and/or the quality of their writing. The only rules are no selling and no competitor put-downs.

The views expressed in this article belong to the author and are not an editorial opinion of Risk & Insurance.