Thank you for the opportunuty to submit evidence to inform the Royal Society’s Cybersecurity research project. I am writing today on my own behalf to draw attention to an easily overlooked set of problems in cybersecurity, aligned most directly with your question 6, “What major cybersecurity research challenges emerging in the next 5-10 years have not been identified.”

Allow me to summarize my perspective, and then expand on each point. The problem, in its simplest form, is that we do not have a good idea of what is going wrong in cyber-security. Lacking a shared corpus of incidents, information about the causes of those incidents, or means of discussing controls, we are unable to assess scientifically if our advice is effective. We lack this shared corpus because we have tacitly agreed to not discuss our mistakes. The reasons for this are worthy of study, and such study should inform efforts to overcome our inability to learn from our mistakes. A better understanding of what goes wrong could better inform discussion of many of the questions put forth in the call for evidence, but I submit that being able to address “what has gone wrong recently” and “how is that changing,” represent an important emerging research challenge, and the Royal Society should consider investing in meeting this challenge. Allow me to expand on each point.

We do not have a good idea of what is going wrong in cyber-security. For example, how many computers were compromised last month and how? We know approximately how many people got sick and with what, and that information is be assessed and gathered in a process which begins manually. Each member of the advisory group has a view, informed by problems they observe, but we lack a catalog of all information security incidents which occurred or those which met some threshhold. We know of some subset as a result of various rules requiring disclosure of breaches which release personal information, but the relation of that set to the larger context is unknown. There is a blind-men and the elephant problem in cyber-security. (In brief, each blind man touches one part of the elephant, and describes it: “it’s like a snake” says the one touching the trunk, “no, it’s like a tree” says the one touching the leg.)

We lack a public corpus of incidents, information about the causes of those incidents, and means of discussing controls. There is no public corpus of incidents. Perhaps closest to a corpus for study are the collections of breach disclosure letters published by some US state governments. After some security breaches, we learn surface information such as “a hacker broke in” or “policy was not followed.” (Sometimes, we also learn that the policy was too sensitive to distribute internally[[1]](#footnote-1).) There are some private information sets, for example, held by CERTs. These are generally not available for academic research, peer review, and in my own conversations with such organizations, the data is not high quality. Information about the hacking technique is rarely forthcoming, even to the level of did the attacker use a vulnerability or convince someone to take action? What controls were in place which might be expected to prevent the attack? Was there a failure to act on information because of too many alarms? A mis-configuration? Did some control simply fail? (Perhaps revealing such information invites additional attacks, but that hypothesis is untested.) Information about the root causes beyond the attack is rarely gathered or shared. (I use the term root causes as few complex incidents have a singular cause.) Without such analysis, it is unsurprising that the same mistakes are made over and over again. Compare and contrast to the state of air travel safety information, where a team of trained investigators will show up to investigate incidents of a certain severity, and then publish their reports for all to learn from.

We are unable to assess if our advice is effective. There are a wide variety of advice for defending a system, ranging from the Australian DSD “top 35” controls, 12 PCI controls, the SANS top 20, and US “Federal Risk and Authorization Management Program” set of 168 controls. Which works better? Which works better for a given level of investment or sort of organization? We don’t know and in many ways, often seem to accept our failure as if the difference is an unsolvable mystery. Some, including members of this project, are working to address this. However, as far as I am aware (as an advisor to RISCS) the data sets are small. The standards bodies that put forth advice often lack even rudimentary feedback loops. For example, PCI is mandated for those accepting credit cards, over a great deal of grumbling. They do not require after-incident reports be filed with the PCI Council, rather asserting that anyone breached was not compliant.

We lack a shared corpus of incidents, root causes or analyses because we have agreed to not discuss our mistakes. The steering group is certainly familiar with the reasons for not discussing security incidents, but we can do better than folk knowledge. The reasons for this are worthy of study. Analysis of disclosed breaches (after the passage of American laws requiring such disclosure) shows that stock price barely moves, and that customers do not flee in droves. (Acquisiti, 2006) A more complete list of reasons why organizations prefer not to discuss incidents would enable study of those reasons, and perhaps help us overcome the reticence. (Of course, it’s possible that simple shame will win out.)

A better understanding of what goes wrong could better inform or interact with several of the questions put forth in the call for evidence:

* In item #2, why security is so often neglected? This should come out in root cause analysis of incidents. (Intuitively the neglect could come from the difficulty of deciding what security investments to make, a result of lacking the ability to decide if our investments are effective.)
* Assessing the efficacy of lessons from item #3 becomes easier if we have a baseline measure of efficacy.
* Many of the questions raised above bring questions about what responsible research might look like in these areas.

Being able to address “what has gone wrong recently” and “how is that changing,” represent an important emerging research challenge. These questions prompt others: Should there a body chartered and funded to gather information about cyber-security incidents? Would research into what methods for analyzing incident root causes generates the best results (and what metrics should be used for assessing best)? There are a variety of methods for sharing or publishing information. What are the tradeoffs between aggregated, anonymized or other approaches?

As such questions are addressed, and more data becomes available, there will be a need to understand its validity over time. Technologists are fond of claiming that “this changes everything.” How important are those changes to security? Can we take lessons from the rise of personal computers and apply them to the current challenges of “bring your own device?” What lessons will transfer from the internet of computers to the internet of things?

The Royal Society should consider investing in meeting these challenges. I would be honored to discuss these questions further.

Yours truly,

Adam Shostack

adam@homeport.org

References

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is There a Cost to Privacy Breaches? An Event Study." In *WEIS*. 2006.

1. http://www.theregister.co.uk/2007/12/17/hmrc\_manual/ [↑](#footnote-ref-1)