Trends in Information Security

Topic Description:
Assessing the Value of Cyber Exercises

Prof. Chris Johnson,
School of Computing, University of Glasgow.
Johnson@dcs.gla.ac.uk
http://www.dcs.gla.ac.uk

Introduction

Cyber-exercises are used by many companies and by government agencies to prepare for future attacks. Staff use these drills to practice the technical skills need to detect, isolate, diagnose and recover from an incident. The exercises often involve managers in simulations that involve difficult decisions – for instance, about resource allocation and communication with external agencies – including regulators, security/police organisations, customers, the media etc. However, a host of open research questions remain – in particular there are questions about the cost-effectiveness of drills. Does participation in a cyber-exercise really help when many actual attacks are very different from the training scenarios? Is it possible to provide participants with a realistic impression of the pressures and constraints that arise when companies begin to lose systems under a real attack?

Different Perspectives

As mentioned in the introduction, there is wide agreement about the utility of cyber-exercises. Even so, many companies do not invest or participate in these drills. The reasons for this can include complacency – why invest in an exercise when there have been no documented attacks on a particular company? Similarly, there is often a concern that by publicising a drill a company might attract the attention of a potential attacker. Further differences of opinion arise over responsibility for cyber-security. Some service providers take the view that the government will ultimately help protect industry from state sponsored attacks. Hence, they will only invest limited resources in exercises and drills unless public funds are used to pay for their participation in a drill. Where there is significant competition in an industry, the costs of holding an exercise must be passed onto the consumer – hence companies that do not invest in a drill may have significant financial advantages over those companies that do pay for these exercises. Companies that under-invest in security will only retain the benefits of under-investment until they suffer an attack.

Open Research Questions

A number of research questions remain open in this area – a partial list includes the following:

- ***How to identify appropriate scenarios for a cyber-exercise?***
  Scenarios are the "story lines" that are used to explain what happens in an attack to the participants in an exercise. It can be hard to identify an appropriate scenario or script because there is a temptation to prepare for the last major attack rather than the next. It is difficult to identify the next possible attack without being able to tell the future.

- **How to Assess an Appropriate Level of Difficulty for a Cyber-Exercise?**
  One aim of a cyber-exercise can be to challenge complacency. This can be done by exposing technical staff to some of the more challenging forms of attack, for instance using the state machine effects in Stuxnet. Similarly, many government agencies assume that most organisations can cope with what are called N-1 contingencies – in which a cyber-attack occurs uner ideal situations. In contrast, they advocate training using more catastrophic 'N-2 scenarios'. For example, the UK banking industry held a drill in which a major cyber-attack occurred at the same time as the London Olympics – when transport was more difficult and key staff were assumed to be on holiday watching the games. Equally, if a scenario is too complex it may disillusion or alienate staff from participating in future exercises.

- **How to Increase Realism and Avoid the Hawthorne Effect?**
  It is hard to recreate the conditions that hold during a real attack. In particular, cyber-exercises can suffer from the Hawthorne effect that arises when people behave differently if they know they are being watched. In other words, during an exercise staff are more likely to follow security procedures and policies than they might otherwise be during day to day operation.

- **What are the Boundaries of a Cyber-Exercise?**
  A host of research questions surround the scope of a cyber-exercise. For example, how many external agencies should be contacted? Do you include customers – judging that they will be confident in a company that conducts such contingency planning or worrying that the mention of an exercise might increase the concern of end users? Hpw long should a cyber-exercise take given the costs of allocating staff and of maintaining the scenario – especially when forensics can take days or weeks to diagnose the attack trajectory?

- **How to Assess the Effectiveness of a Cyber-Exercise?**
  Above all, questions remain about the metrics that might be used to assess he effectiveness or utility of cyber exercises. There seems little evidence to show that companies that participate in these drills respond better in the aftermath of a real attack. One of the reasons for this is that each attack tends to have unique characteristics that prevent us from making such simplistic comparisons. Equally, it seems clear that there can be 'good' as well as 'bad' exercises – so how can we tell if we are spending our money wisely when we hold one of these drills?

Note if you are interested in this area then contact Arniyati Ahmad arniyati@gmail.com who is completing her PhD in this area.

References

Dodge, R. C., Hay, B., & Nance, K. (2009, March). Standards-based cyber exercises. In Availability, Reliability and Security, 2009. ARES'09. International Conference on (pp. 738-743). IEEE.

Furtună, A., Patriciu, V. V., & Bica, I. (2010, June). A structured approach for implementing cyber security exercises. In Communications (COMM), 2010 8th International Conference on (pp. 415-418). IEEE.

Mattson, J. A. (2007, January). Cyber Defense Exercise: A Service Provider Model. In Fifth World Conference on Information Security Education (pp. 81-86). Springer US.

White, G. B., Dietrich, G., & Goles, T. (2004, January). Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 10-pp). IEEE.

Branlat, M., Morison, A., & Woods, D. (2011). Challenges in managing uncertainty during cyber events: Lessons from the staged-world study of a large-scale adversarial cyber security exercise. In Human Systems Integration Symposium (pp. 10-25).

Grimaila, M. R. (2004, October). A novel scenario-based information security management exercise. In Proceedings of the 1st annual conference on Information security curriculum development (pp. 66-70). ACM.