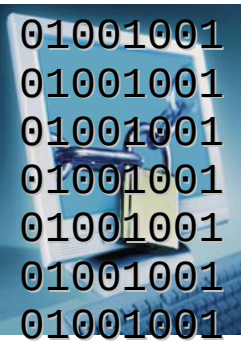
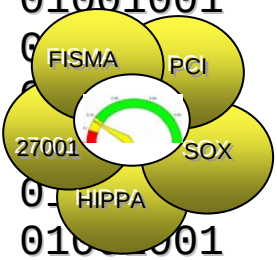
HAMPTON ROADS
TECHNOLOGY COUNCIL
IT FORUM



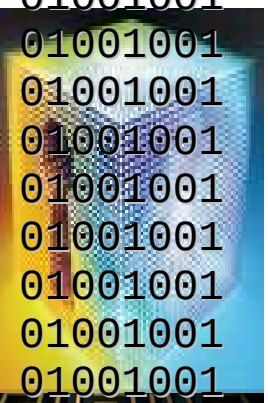
Computer Security Incidents:
Elements of Good Decision Making

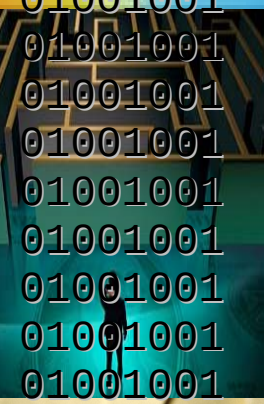


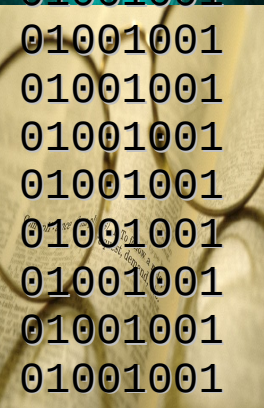
If a computer security incident were to occur, would you recognize it? Do you know who to call, what to do, and in what order? Under-reacting and overreacting can both be devastating, so how do you know? Planning for the right amount of response using the right procedures for a computer security incident can be like a beacon in a storm.

HRTC and the IT Forum invite you to learn from an Industry Expert:

- How to reduce your risks and support your recovery after an incident
- Explore real examples of how a small planning investment delivers big returns
- Introduction to the most common tools and methodologies used by a Computer Security Incident Response Team (CSIRT) during the lifecycle of an incident
- Discover the capabilities of local industry to support your IT Security and Compliancy Needs
- Collaborate with other local IT and Business leaders facing similar challenges







DATE/TIME: 10:30AM-1:30PM, 11 Oct 2007
LOCATION: Holiday Inn Select, Norfolk Airport
REGISTRATION: http://www.hrtc.org/en/cev/?8

SPECTRUM
ENVISION THE FUTURE

HAMPTON ROADS
TECHNOLOGY COUNCIL
IT FORUM

This seminar is brought to you by Spectrum,
A local instrumental in the planning, design, implementation, and maintenance of our government's Intelligence Exploitation Systems

HRTC And The IT Forum Would Like to Thank The Following Sponsors and Participants:

SPECTRUM
ENVISION THE FUTURE

7W Queens Way
Hampton VA 23669
757-224-7500 Voice
757-224-7515 Fax

If you would like to parcitpate in the HRTC IT Forum please contact:

Russ Herrell
Rherrell@windwardcg.com
757-214-8744

Rob Floodeen is an Information Security Architect for the Hampton, Virginia based Spectrum Comm Inc. He is leading several projects for Spectrum's new Envision Labs division which will revolutionize approaches to Risk Assessment, Intrusion Detection, Incident Response, and Attack Sensing & Warning. Rob is an expert in information security policy analysis, developing guidance on emergency preparations, and providing hand-waving-over-simplifications. When time and schedule permits he also works as a Visiting Scientist for Carnegie Mellon's (CMU) Software Engineering Institute (SEI).

Before joining Spectrum, Rob has led teams performing Intrusion Detection for the likes of the Pentagon, Army Research Lab, Defense Research and Engineering Network (DREN), and was an Operations Manager for a DoD Agency Computer Emergency Response Team (CERT).

Summary: Computer Security Incident… Hopefully, not three words you hear every day. But if a computer security incident were to occur, would you recognize it? Do you know who to call, what to do, and in what order? Under-reacting and overreacting can both be devastating, so how do you know? Planning for the right amount of response using the right procedures for a computer security incident can be like a beacon in a storm.
If there is information anywhere in your value chain, then some prudent planning up front can make all the difference. We'll talk about some of the practices you can put in place in your business to reduce your risks and support your recovery after an incident. We'll look at some of the most common planning elements that go into incident response and recovery plans. There are many prudent steps you can take now, that cost little or nothing, which make your chances of weathering a computer security incident. We'll illustrate examples of how a small planning investment delivers big returns.
Once you've committed to a plan, what tools and technology do you need? Here too, risk can be reduced for little cost. We'll introduce the most common tools and methodologies used by a Computer Security Incident Response Team (CSIRT) during the lifecycle of an incident. You should find approaches for protecting your business.
This high level overview will be valuable for anyone who is responsible for or manages IT infrastructure.