



A New Security Environment

March 2008

Nat Heiner

CTO, Northrop Grumman IT Defense Group
Enterprise Infrastructure

nathaniel.heiner@ngc.com

Satellite Technology
Information Technology
Nuclear Aircraft Carriers
Unmanned Systems
Missile Defense
Space Systems
Intelligence, Surveillance and Reconnaissance
Navigation Systems
Systems Integration
Shipbuilding
Electronic Systems
Radar and Air Defense

Typical Enterprise Infosec Posture

- **It's bad out there: our networks are intact, but under constant attack, always at risk of penetration or spillage**
- **We practice network defense in depth**
- **We have clear policy, and we know what to do if there is a security event**
- **We are constantly looking for ways to improve our defense**
- **We certify our security people**
- **We have a 7/24 network security team, and a response team ready to go**
- **These teams are aware of emerging threats, and in contact with appropriate partners in the network of security analysts**
- **We train all employees in security awareness**
- **Although we support military and intelligence customers, we have segregated our corporate networks completely from theirs, to ensure complete air-gapped independence**

Questions to Consider

- It's bad out there: our networks are intact, but under constant attack, always at risk of penetration or spillage

How do we know they're intact? Is it not possible that something might be lurking quietly in our network? How do we prove this impossible?

- We practice network defense in depth

Is defense enough? Are we rigged for attacks from within?

- We have clear policy, and we know what to do if there is a security event

Do we have a regular exercise plan? If so, how do we disseminate lessons learned, or ensure that lessons really are learned? What organization has responsibility and authority to ensure this?

- We are constantly looking for ways to improve our defense

How often do we add new tools to our kit, how often do we retire older-generation tools? What is our process for keeping our security people connected, educated, on edge?

Questions to Consider

- **We certify our security people**

How do we know these are the right certifications? Do we have an ongoing scan to verify that emerging standards are in the certification mix? How do we overcome the built-in staff inertia driving a preference for those with certification just like our own?

- **We have a 7/24 network security team, and a response team ready to go**

Is there segregation of duties among these teams? How do we exercise them?

- **These teams are aware of emerging threats, and in contact with appropriate partners in the network of security analysts**

Do we have a team of dedicated analysts, or people who know how to engineer honey-nets on the fly in response to an immediate threat?

- **We train all employees in security awareness**

How do we measure what they have learned? By a test right after annual training? Is that really a measure? Given the stakes, is there another way?

Questions to Consider

- Although we support military and intelligence customers, we have segregated our corporate networks completely from theirs, to ensure complete air-gapped independence

How do we know they are really separate?

Is there any way that penetration of one of our corporate networks could open a vulnerability to one of our military or intelligence customer networks?

Could an NGO penetrate NIPRNET in order to steal highly sensitive corporate secrets? How do we know this is not possible?

Is it possible that we really are all connected?

If so, how do we continue to execute our missions reliably, despite our nagging doubts about the perfect intactness in our networks, data, and systems?