


IT Security Challenges for Distributed Science




Douglas Gatchell
National Science Foundation
Office of Cyberinfrastructure

FedCASIC

March 16, 2006

March 16, 2006 Douglas Gatchell Slide 1

Good morning. I'm Doug Gatchell. I'm a program director in the Office of Cyberinfrastructure (OCI) at the National Science Foundation (NSF). NSF provide funding support for basic research in all areas of science. As a general rule we do not provide funding for applied research (I.e. research that is likely to directly result in a marketable product). We also fund infrastructure that is required to support basic science research. Infrastructure includes networks, computers, data storage, software tools, and IT education. Over the years our basic science projects (like: physics, atmospheric research, ocean science, earth science, and environmental research), have become increasingly dependant upon information technology. Our support of general use cyberinfrastructure, like computational resources; has become more distributed, more fundamental and necessary and more expensive. We have, by necessity begun to share our resources not only with other science agencies in the US but with foreign scientists all over the world. Science is truly a global effort and collaboration, communication and sharing of resources is critically important.



Outline

- What do we mean by IT Security?
- Why is NSF interested in IT security?
 - Represent investment of large amounts of Federal funds
 - IT security is hot topic
 - Security is important
- What can NSF do?
- What does NSF expect of its awardees?

March 16, 2006 Douglas Gatchell Slide 2

Today, I want to discuss and why the National Science Foundation is concerned with IT security. And I would like to talk about what we are doing about it and what we will expect from those we support and those we share our resources with.

When I talk about Security of our Information Technology assets, I mean we want to make sure those assets are used for their intended purpose. We especially don't want those assets used to support attacks on our critical infrastructure. Secondly, we want the infrastructure to be available when scientists and educators need it since outages can result in missed opportunities and loss of productivity. Finally we want to make sure the integrity of the data and communications is preserved and protected.


Everyone is familiar with IT security these days from the average home user to the universities presidents who must now worry about liability issues related to privacy and piracy problems.

Sometimes the priorities are in conflict. For example, security may require knowledge of who is accessing resources. Privacy requirements

may require the unique identification information not be maintained without onerous and expensive safeguards. I will talk not only about process issues but cultural and organizational issues that make providing cybersecurity a great challenge for all of us.

NSF

Global Communications Distributed Science



March 16, 2006 Douglas Gatchell Slide 3

Security is important to everyone but it's a difficult nut to crack because in our distributed science community no one has control over the distributed user community. We rely on making our resources available to people in other domains managed by others. This is complicated by different priorities, different languages, different time zones and no formal agreements.

NSF can work with our grantee community to make sure they understand their responsibilities to providing and promoting good IT security practices. We can encourage communications and cooperation.

NSF will start making "good" IT security practices a requirement of grant funding on all infrastructure projects. Grantees will be reviewed and evaluated on their efforts to meet IT security guidelines.



Threats

- Viruses
- Worms
- Malicious software downloads
- Spyware
- Stolen credentials
- Insider Threat
- Denial of service
- Root kits
- Session hijacking
- Agent hijacking
- Man-in-the-middle
- Network spoofing
- Back doors
- Exploitation of buffer overflows and other software flaws
- Phishing
- Audits / Policy / Compliance
- Power failure
- Fire
- Natural disaster
- Social engineering
- ????



March 16, 2006
Douglas Gatchell
Slide 4

There are numerous threat vectors which can nail your systems including: corruption, denial of service, recovery, misuse. Have you looked at your environment with respect to threats? Are you ready?

In 2004 an unauthorized and unprecedented intrusion into numerous university and federally funded research computer systems was discovered. Before it was over there was a cost of billions of dollars worth of time and compute resources. Fortunately little data was lost or corrupted.

Since technological solutions have evolved so fast over time, security has lagged and was not part of the technology revolution culture 20 years ago. Today security is often practiced in an ad-hoc manner by people who are quite competent but narrowly focused.

Many of the NSF facilities are on the high performance research networks. A break-in at any of these facilities potentially puts others on the network at risk. NSF want to make sure the facilities understand their responsibilities and the need for security policies and plans.



For IT security – the time has come.

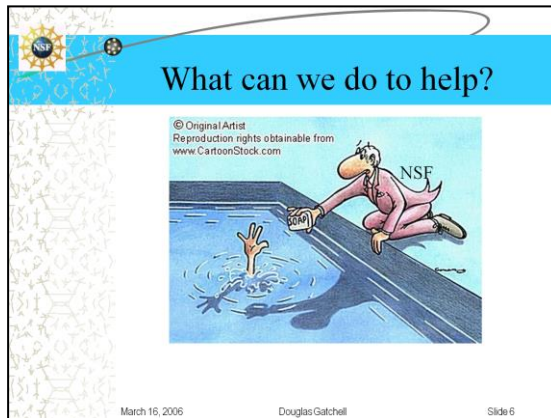
Over the years we have exploited technology as a tool to help us work more efficiently and effectively. Today we rely on information technology to get our work done. This has been gradual and has occurred without much planning. Not only can the loss of this technology become a serious business problem resulting in data loss or corruption, it can cripple a facility and cause staff to lose many hours. As if this wasn't bad enough, there is a growing awareness the systems and networks we use in our home, office and laboratories can actually be compromised and used to launch attacks against IT assets outside of our institutional domains.

Some businesses, like those in the financial sector, have always been aware of the need for security but they too are becoming increasingly reliant on the Internet for doing business. A general failure on the broader Internet could result in significant economic losses for everyone.

Current security activities are primarily **reactive**. Security planning should begin at system design and installation. There is a need for better intrusion monitoring and logging and a need effective and efficient forensic analysis. Many of these can be served by **automated tools**.

Grid computing amplifies existing security issues, rather than creating new ones.

e.g., local sites are likely to strengthen firewalls to meet increased security risks which may result in reduced performance, accessibility problems and process failures.



What can NSF do to help?

We must recognize and understand the needs? We need to respond to those needs appropriately. This includes recognizing that every site, every institution, and every situation may have different needs. One size does not fit all!

At NSF we have many complicated guidelines on appropriate spending for federal funds. There are many checks and balances on how both the government agencies and our grantee community can use award funds. Records must be meticulously maintained and institutions are subject to frequent audits. Perhaps the same sort of guidance can be provided for IT security.

Based on guidelines developed by the US National Institute of Standards (NIST) we have identified seventeen (17) principals we believe each site should address in developing their own approach to IT security. These guidelines are in draft form currently because they haven't been reviewed or accepted either by the agency or the grantees. Many of these points overlap so I won't dwell on them, but a review will give some idea of what we consider important.

 **Minimum
IT Security Requirements**

**Draft Federal Information Processing Standards (FIPS)
Publication 200 "Minimum Security Requirements for Federal Information
and Information Systems"**

1. Physical Access Control
2. User awareness and training
3. Audit and Accountability
4. Certification, Accreditation and Assessments
5. Configuration Management




March 16, 2006 Douglas Gatchell Slide 7

- **July 15, 2005 -- Draft Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems***
2. Perhaps the hardest part of security is user awareness and education. If a user doesn't understand the processes or policies or doesn't understand the importance of backing up their data, choosing good passwords or being skeptical about opening unsolicited email, there is little that can be done by the organization to provide adequate security. Recently the Inspector General (IG) for the Commerce Department did a random audit of users and managers of the IRS. By posing as helpdesk technicians the IG was able to convince around 50% of the people to change their passwords to something the inspector could use to gain access to their account.
 3. Facilities should be able to audit who is using their systems and detect unauthorized use. Records maintained can be used not only to trace user actions but also serve for

identifying corruption, intrusions, and provide information required if law enforcement action is required.

4. Because the nature of our computing environments is constantly changing, it is important that facilities have plans in place to monitor and audit compliance and procedures for correcting deficiencies.
5. One of the difficult parts of security is understanding and maintaining control over the resources. Security patches provided by vendors may break existing applications or user procedures. Patches need to be applied but side-effects of these changes may have cost impacts as well. Procedures should exist to track changes and detect problems due to maintenance activities.

 **Security requirements cont.**

6. Contingency Planning
7. Identification and Authorization
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security



March 16, 2006 Douglas Gatchell Slide 8

6. There should be plans and procedure in place to insure there is continuity of operations in the event of an emergency. This may include things like off site backups and disaster recovery plans.
7. Access control can also be logical requiring authentication and authorization before a user is given access to a given resource be it computational power, storage, network, data, etc. The technology or processes used to support authentication and authorization should be proportional to the risk of losing the resources involved.
8. Every site should know what to do and who is responsible for which activities should an incident or intrusion occur. If you discover that you have been attacked will you have the logs to aid the investigation and potential prosecution of the hackers? Incident response planning should include procedures for:
 - Auditing and gathering of information

- Forensics for determining damage and methods of exploitation
 - Gathering evidence for the purposes of law enforcement and potential prosecution
 - Communications with users, managers and other sites on the network
 - Recovery of resources
9. If security was easy we wouldn't be talking about it right now. Maintenance is also important and appropriate procedures must exist to allow changes to be made and tested in a safe environment.
 10. In science, data is often the most important product. It must be protected and backed up. Of course, data is often something you don't want to share with others. It is necessary to consider this when replacing equipment. Procedures should exist to destroy or sanitize data storage before is disposed of or reused for other purposes.
 11. The physical environment can also threaten our infrastructure. Floods, earthquakes, storms and power outages can also have disastrous effects if they occur at the wrong time. Facilities should consider the physical environment when planning their hosting and recovery infrastructure.
 12. Security program is dynamic, constantly changing and evolving to meet different needs and different threats.
 13. Facilities should ensure their employees are trustworthy. They should consider procedures to follow when personnel actions, such as terminations occur. They should also employ formal sanctions when individuals fail to comply with security policies and procedures.



More security requirements

System Acquisition Approach -1

"We Got it Covered" Approach

What software? I am buying a system – my contractor will take care of all of the implementation issues!



14. Risk Assessment

15. System and Service Acquisition

16. Systems Communications Protection

17. Systems Information Integrity




March 16, 2006

Douglas Gatchell

Slide 9

14. Risk = Vulnerability x Threat x Asset Value

Risk analysis is generally considered the heart of the security program because it's an accepted method for deciding where to allocate resources based on the assets that need the most protection.

Risk: Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.


Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.

15. Purchasing plans should include evaluating security, maintainability and life cycle considerations for equipment,

software and services. They should ensure vendors and providers are using good security practices when purchasing decisions are made.

16. Monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems
17. Facilities should have processes to identify, report and fix problems in a timely manner. There should be procedures in place to protect data resources from malicious code and unauthorized changes to data should be detected and reported.



Security approaches clash of culture

- Law enforcement (control)
- Financial (risk management)
- IT (customer service, feature rich, technical)

March 16, 2006 Douglas Gatchell Slide 10

Security means different things to different people. You've probably heard the old saying "to a carpenter with a hammer every problem looks like a nail." Well with IT security I can think of three different types of approaches, each of these in potential conflict with the other.

- When the IT security responsibility comes from the folks responsible for physical security, they tend to take approaches which limit and control access to equipment and information. The law enforcement approach will generally result in good prevention. It will also tend to annoy users and limit functionality of systems.

- A financial oversight approach is employed when the CIO or CFO is responsible for IT security. The security approach will tend to be risked base with bottom line decisions being made to minimize organization exposure to financial risk and negative publicity.

- When an IT professional is placed in charge of IT security, the focus is likely to be on customer service and support issues. The approach will favor technical solutions and availability of IT resources even if security risks are evident.

- These approaches can all have good impact and success but they will also clash and create dissidence within the organization, no matter who is in charge. In many organizations such as ours, the CIO is part of the financial directorate which also includes responsibility for IT security and IT support services. So the CIO needs to have multiple personalities.

 **We need to change!**

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**"I wouldn't say my computer skills are outdated.
I prefer to think of them as 'classic'."**

GLASBERGEN

March 16, 2006 Douglas Gatchell Slide 11

Cultural changes, overlapping ubiquitous computing and heightened awareness are changing the way we have to deal with IT security and accelerating the urgency of protecting the resources.

We already know a lot about what make a good security program. Everyone here knows that you need to backup critical data incase of a catastrophic loss. We all know that we shouldn't share our passwords and we should choose good passwords that can't be guessed. We know we shouldn't use the same passwords on different accounts. We know we shouldn't use an email password that is the same as our login password. We know we need to look at our security logs and we know we need to make security a priority. Yet – do we always follow what we know?

NSF


We need to communicate



March 16, 2006 Douglas Gatchell Slide 12

A major problem with security is that our actions or non-actions may impact neighbors we connect to. For example a misconfigured mail server can be used to send SPAM by remote users which will probably not affect the local site at all. Some issues with DNS can result in the ability of remote hackers using a site's name server to spoof sites (i.e. pretend to be amazon.com or bankofamerica.com).

When security events occur sites need to communicate in an efficient secure way to share information to limit the extent of damage. It will often require coordination between sites to track down the attacker and shut off their access.



Realistic IT Security



**“Yes, you’ve done an excellent job of keeping our computer safe.
But sooner or later you’ll have to plug it in.”**

March 16, 2006 Douglas Gatchell Slide 13

OK – Realistic security is hard.


Users need training and tools to help them do the right thing. Most people can not remember all the passwords they have to deal with – particularly if they are treating IT security responsibly and not using the same password on different accounts.

But to think people are going to change is probably a bit naive and having a policy may not really accomplish much. We need to recognize the fragile nature of our environment and do the right thing.

NSF

Copyright 2004 by Randy glasbergen.
www.glasbergen.com

Tradeoffs



“Sorry, Jim. Due to tightened security measures, we can’t let you in the building with a sharp mind.”

March 16, 2006 Douglas Gatchell Slide 14

Security may require making tough choices. Don't let those choices become damage your intellectual and creative capabilities.



The end

This is a lifestyle change for our culture. The way we approach our work needs to include considerations for security and privacy.

Everyone must be part of the solution, it's no longer a task that can be handled by the central services organization.

Security must be rational...