SAND2000-0663C

RECEIVED
APR 04 2000
OSTI

Security Issues at the Department of Energy and Records Management

Anna W. Nusbaum, CRM
Records Management Officer, Sandia National Laboratories

The fine print:

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Besides our usual funding statement I need to put in this disclaimer. Any of the discussion about the "history" of events prior to the security shutdowns and of the amazing project are purely from my own perspective and do not necessarily reflect the perspective of Sandia National Laboratories nor of the Department of Energy.

Some Background

In order to discuss the connection between security issues within the Department of Energy and records management, I'll need to cover a bit of security history and talk about what I call "the Amazing Project". I'll describe why I think this project was so amazing and what it accomplished. There's a bit of sad news about the project, but then I'll move on to discuss what we learned at Sandia as a result of the project and what we're currently doing in records management.

In the beginning, nearly everything created at Sandia was "born classified" - almost all the technical work we did was related to weapons. Over time, especially since the late-seventies, the perceived importance of being born classified declined. Sandia picked up other missions from the Department of Energy, many of which were either not classified or "not as classified", thus creating a mixed culture of weaponeers working in the area of national security and engineers and scientists working on renewable energy resources, waste management, and cooperative research and development projects. People transferring to the weapons area brought a different experience and expectation of how to manage the security of information and that collaboration was a good thing.

At the same time, recurring budgetary reductions and increasing pressures on reducing overhead specifically drove Sandia (and the other sites) to seek alternative solutions to physical and information security, often with unintended consequences. Installing automated gates to replace the labor force of live security police created an impression that one could relax more about what you took home. Later in the eighties, openness initiatives by the White House and supported by the then Secretary of Energy added to the local impression that classified was not only not important, it was a liability. Resources for computing were applied to the external and internal unclassified networks. All the really neat applications and tools were on those networks and the processes for certifying applications for the classified network became slow and cumbersome, driven by reduced resources and the desire for increased oversight. Finally, the Internet just boomed - working electronically became the fast and convenient way to collaborate without incurring travel costs and losing time. A highly competitive business environment within and external to the DOE with extremely short turnaround times helped to create an information environment that made it easy to live in the yellow restricted network.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic Image products. Images are produced from the best available original document

Then, one day in 1998, an individual brought a package to a CIA office in Europe and a lot of things happened pretty fast, including shutting down the laboratories for intensive security training and awareness. The first shutdown happened, coincidentally, when I were at last year's ISG midyear seminar in Georgia!

As you might imagine, it's pretty embarrassing to be accused of releasing national secrets, especially if they have to do with nuclear weapons. While I cannot talk specifically about the case, I can relate what's been in the papers. The documents that were delivered looked like they came from one of DOE's national laboratories and eventually the cloud hovered over Los Alamos National Laboratory and upon the gentleman currently residing in a New Mexico jail.

All kinds of studies were commissioned and all kinds of fingers were pointed at all kinds of people, programs, and agencies. At one point it was allowed that most of the documents could have come from any number of other agencies. The Department of Energy clearly needed to act quickly and have the Nuclear Weapons Complex respond quickly and the Six Points and Nine Action Items were delivered with rapid implementation schedules. The "6 plus 9" as they came to be called are below.

Secretary of Energy's Six Points

Here are the six points. Sandia had direct responsibility for number two and five - the Department of Energy had responsibility for the other four, which still had consequences for all the Nuclear Weapons Complex sites, including Sandia.

1. DOE sites will establish a program to continually monitor computer systems for security.
2. DOE will establish an aggressive Department-wide cyber-security-training program using mobile training teams.
3. DOE will conduct random audits of individual computer users to ensure compliance with proper security procedures.
4. The new Office of Oversight and Performance Assurance will establish a program of continuous independent oversight of cyber security with support from the Office of Counterintelligence.
5. DOE sites will make better use of technology to combat the hacker and espionage threats.
6. DOE Orders regulating downloads from classified computer systems will be enforce and compliance will be verified.

Department of Energy Nine Action Items for the Weapons Laboratories

Here are the Nine Action items. Just give these a quick glance and think about how your site would go about doing these things in a matter of weeks! The nine action items were to begin implementation April 1, 1999.

Item one: Within seven days each lab will schedule a security suspension of al classified personal computers (exclusive of computers performing safety or security functions). During the suspension, professional and administrative staff who would normally use these computers will be required to attend training and review sessions in computer and information security policies and procedures.

Item 2: On a continuing basis, each lab will institute aggressive computer security training and threat awareness for all personnel who use classified computers.

Item 3: Within 14 days, each lab will make it physically impossible for classified information to be moved within a single work area from a classified computer to an unclassified computer by the transfer of removable media (tapes, disks, etc.).

Item 4: Within 14 days, each lab will put into force rigorous new procedures governing the authorized transfer of unclassified files from classified computers. These procedures will require both (i) that persons authorized to transfer files be current in the Personal Security Assurance Program (PSAP) personnel reliability program, and (ii) explicit two-person physical control of all transfers.

Item 5: Within 30 days, each lab will audit unclassified computer systems to insure compliance with procedures for control of sensitive information and will put in place automated sniffing/monitoring programs that continuously scan for classified content in unclassified storage archives and outgoing e-mail. Summary audit reports will be transmitted to the laboratory directors and to the Secretary of Energy.

Item 6: Within 30 days, each lab will more stringently apply need-to-know criteria to classified data archives, and will institute automated means to monitor and enforce access policies, and to deter and detect any violations.

Item 7: On a continuing basis, starting immediately, each lab will take technical measures to increase the security of its classified networks against insider threats. The specific measures were discussed in a classified attachment.

Item 8: Each lab will move rapidly to complete its three-level network protection program and will implement intrusion detection systems at each level.

Item 9: Each lab will institute continuing vulnerability analyses, including the use of red teams and senior technical computer policy boards.

The Amazing Project

In the Spring of 1999, an individual in the Weapons Program office of the DOE Headquarters commissioned a project that I call "the Amazing Project". Initiated in late May 1999, it was to be a tri-laboratory (Lawrence Livermore National Laboratory of Livermore, California, Los Alamos National Laboratory of Los Alamos, New Mexico, and Sandia National Laboratories of Albuquerque, New Mexico, and Livermore, California) project. The team that formed was tasked to develop the best set of security solutions that still enabled weapon mission work to get done and the security solutions were to be the same set for everyone. The amazing project was called "The Integrated Security Management Project", or "ISecM" for short.

Why do I think the ISecM project was so amazing. While it wasn't the first time these three laboratories had worked together, it does represent the first time the laboratories were

working together for a common goal and a common solution that each lab would then live with. It was also amazing in that a process for delivering upward input for changes at the DOE Headquarters level was in place and ostensibly agreed to by HQ. It was additionally amazing because the Nuclear Weapons Complex production plants in Pantex, Oak Ridge and Savannah River were pushing to be included earlier rather than later. Finally, the most amazing thing about this project was two components that represent "impossible dreams" to most records managers looking at the typical technical project. One, there was a management component in the project that would be responsible for addressing, designing, and implementing the needed management processes for integrated security. Second, there was actually an Information Management component directed at analyzing, enhancing, simplifying, revising Information Management elements.

ISecM Project Accomplishments

So, what did the ISecM Project manage to accomplish? There were two stages to the project. The first stage was to deliver a study on what it would take to achieve pre-eminent cyber-security while enabling world-class science and engineering in the Nuclear Weapons Complex of DOE. The development of that study, comprising an expanded team of nearly 50 people, occurred over the summer of 1999. We affectionately called that the "summer camp". It represented many, many hours of proposals, arguing, often passionately, about what it would take, what could be done, what couldn't be done, how could it be done, why couldn't it be done, and how would it be phased? During the summer, the original tasking individual at DOE would modify the scope of the project (all DOE versus just the NWC; all information vs electronic information) but never the result - pre-eminent cyber security that still enabled the work to get done. The team was told to think as clean a slate as possible in order to achieve the right things.

The report was completed at about 10pm up at Los Alamos National Laboratory on August 31st. A team member borrowed my rental car, drove the three copies of the report to the parking lot of American Furniture where he met another team member who got on the 8:40am non-stop from Albuquerque to Oakland to hand deliver the report to the sponsor on September 1. All during the summer none of the team and especially the team leadership and the advisory committee to the team made no bones about the fact that the schedule was aggressive, that what was demanded resulted in innovative architectures and processes, and that the result was going to be very, very, expensive.

The requesting sponsor gave the go-ahead, without any additional funding, to begin planning the project specifics: developing a detailed work break down structure, organizing the efforts into 8 major areas, including the management and information management components, and to start looking at timing, costing, and resource needs. The Department held a briefing for interested vendors the week of Labor Day in Washington, DC, indicating that there would be room at the table for vendor participation up to and including a turnkey solution. Interested vendors were invited to show their stuff at vendor briefings in California the first week in November.

From September through the end of October, we met frequently, in-between encrypted e-mail correspondence, to hammer out schedules, task details, descriptions, resource needs,

purchases, etc. From September through the end of October, no additional funds were coming from DOE to pay for this effort - each lab and plant was scrounging for $$ to cover the labor and travel. Finally, during the week the vendors were briefing us on how they thought they had solutions for the project, the project was suspended. We went home.

Learning that the project was suspended was like having a death in the family. It was awful.

Moving on.

What did the ISecM plan propose for Information Management? From the project plan:

> The purpose of Information Management in the Information Security Management Program was to develop the standard frameworks (e.g., sub-policies, requirements, procedures, training) for IM processes and standard IM tools (e.g., web-based information, decision charts, information management plans, mobile media controls, classification checker).
>
> These standard frameworks and standard tools were to enable managers and users to:
> - Understand the threats and corresponding protection measures; thereby contributing to reduction of insider threat
> - Understand the value of the weapons information (information as an asset)
> - Effectively protect the information while executing DP mission work and other DOE funded work, and while collaborating with other agencies, universities, and companies.
> - Invest in the special certifications needed for employees with critical access responsibilities
> - Make informed information management decisions with respect to "where" information is born and lives, how long to retain, migration, and how to safely release
> - Find the Agency secure Network (the red, classified network) and Site Restricted Network (the yellow, internal/sensitive network) the "systems of choice" for their classified, sensitive unclassified nuclear weapons information, and other sensitive information management needs.

There were three planned components for Information Management:

Training:

- Integrated training for all constituents required annually, that covers the basic life cycle management concepts, current risks and threats, export control issues, basic protection principles, information release processes, and Agency Secure Network (ASN) & Site Restricted Network (SRN) features. Included will be reference resources "for more information".
- Specific modular training for special topics. The need for these topics will be role and responsibility driven, such as for employees with critical access; program managers, foreign travelers, hosts for foreign visitors, and will cover those detailed information management topics and detailed "classified life" topics that are pertinent.

Information Management:

- Information Planning framework and tools that will permit managers and employees to incorporate information life cycle needs into their programs and projects and then exploit the functionality of the ASN and SRN to make it "easy"
- Standardized Document Management Processes: managing the information on the ASN, SRN, and Site Open Network (SON) (creation, sharing, protection, retention, migration, back-up, metadata).
- Standardizing (and simplifying to extent possible) classified and sensitive information management policies and procedures and making the management of classified in the cyber and physical world logically consistent.

Classification Simplification

- Create" classification primers" and place on line. These primers, organized by programmatic or topical area, will, succinctly, discuss what information is covered in a topical area and what the boundaries are for keeping the information unclassified, sensitive, or classified.
- On-Line Support Tool for Classification Assistance. An online, user-friendly classification support tool that provides authors of documents basic information on what is and is not classified. It will contain, among other features, a "spell-checker" type devise that can identify what MIGHT be classified as text is generated.
- Strengthen and standardize training for ADCs and managers.

Lessons Learned

So, what did we learn from the security activities in the records management program? First, that awareness is essential. People are generally inclined to do the right thing (1) if they know what it is and (2) if it makes sense to them. Awareness helps folks know what the right thing is.

Second, that coordination is critical. Making sure that one program at Sandia doesn't do something that contradicts what another program is trying to do goes a long way for having processes make sense. So, the right hand has to work with the left hand to have that happen. Protecting information while ensuring appropriate and continued access to that information is a key element of both the records management function and the security function.

After all, what is it that a site or company protects? Its people, its physical and financial resources, and its information! Without those critical elements, what does a company have to work with?

We also discovered that not only could the records management program NOT perform this magic alone, it didn't have to! By integrating our efforts with those of the information systems programs and with security, we can deliver a much more powerful and integrated message. We all, then, can tell, train, share, and help our customers with a common message and create a stronger and more confident customer base as a result. We also, together, can challenge the stupid stupid processes, the stupid rules, and the stupid policies. The goal is to move from "customer tolerance" to "customer acceptance" to "customer champions", because

at that end stage, the customers perceive all of us as being a value-added element in their work and processes.

What are we doing now?

How are we carrying on the "legacy", if you will, of what we learned during the course of the amazing project? We are redoubling our already successful efforts with Information Systems and Security. We're working on integrating our records management training with computer security this year, for example. And, we're participating on a Corporate-wide committee looking at all the required training to see what can be consolidated.

We've worked with the Y2K team, so that records management and records retention was part of the project efforts, including making sure system administrators were aware of a web-based document management application was available to store their Y2K records.

We enjoy a great reputation and rapport with our customers and believe a strength we bring to these partnerships is that of messenger and facilitator, tying the other activities together.

Our records management program believes in using the "power of three":

1. We need to drive change, or it will mow us down.
2. We need to integrate our policies and procedures, so that they make sense, give a common message, and are easy to understand and follow.
3. And we must use the KISSS principle - above all, Keep It Simple, Smart, and Secure!