



**[PHILLIP LORANGER:]** This is kind of what we're going to cover today. I'm going to cover threat, and I'm going to cover the threat and so forth in an unclassified format. It's a little more sexy with the classification piece, but it's really important to Bob and I to start some information sharing in the line of threats, cyber security, cyber exploitation, those kind of things, with our primary customers, which is you all here. So I'm going to talk about threat, talk about tools and services that are being used out there, organizations that are attacking us, and where we might be able to protect ourselves a little bit better.

Now, have any of you ever hacked legally? Illegally? Oh, I can't believe that. This is maybe the only presentation I've ever done that there's not someone in the room that hasn't used someone else's password. Has anybody ever done that? No? Well, there you are; if you've done that, you are now a hacker, because you were not an authorized person using an authorized access mechanism to get into an authorized system. Ever met a hacker? Ever talked to a hacker group? Ever had a hacking demonstration? No? You have. Where at?

**[AUDIENCE:]** [ Inaudible ]

**[LORANGER:]** Well, good. For the rest of you who haven't, you have now. I was one of the first, way back when my hair was past my shoulders, hacked the Senate Science and Technology Subcommittee, only because the chairman told me I couldn't, so we showed to him that we could. Also took care of the Adjutant General of the United States Army, made him an executive assistant and made his pay equal that. He was not a happy camper. Also promoted a few friends of mine to brigadier general that were on the '06 list. So a lot of cool things. What I've never done, though: I've never hacked the school and changed my grades because no one would believe if I got anything above a C anyway. I won't talk about that.

The threat today is very, very real and very, very serious. If you're just watching *60 Minutes* or *20/20* or reading the paper and so forth, you'll see it. I'm going to share the name of a group which has made the unclassified press, so I'm not divulging anything. It's called Russian Business Network. The Russian Business Network is a coalition of cyber criminals, is the best way to describe them, and they do 3 things extremely well to the tune of, last year we assessed they made about \$3 billion. That's dollars with a B. And what areas do they specialize in? Kiddy porn (I'm not going to talk about that today), identity theft, and money laundering, and money laundering in the sense of pretending to be someone that has an account that has some money attached to it. You may have remembered not too long ago, over a long holiday weekend, a federal holiday weekend, there was \$10 million stolen from a number of banks across the nation. \$10 million is not much money -- well, it is to you and I, but not much money in the scheme of banking. And this was so well executed, it was executed by literally thousands of computers, and every one of them just stole a little bit, \$5, \$25, \$50, but they all went to one cyber crime organization. It's like Jesse James. They used to ask him, why do you rob banks, and his answer was, that's where the money is. That's what they are attacking. It's very profitable. Cyber crime and terrorism, we put those on



START HERE  
GO FURTHER  
FEDERAL STUDENT AID®

the same line because both of them are criminal activities, but I will share with you on the terrorism side and why I even bring terrorism and terrorism groups into this discussion today in the threat scenario. We, and when I say this, it is the intelligence community, which I work with, have actually recovered notebooks and stuff out of caves in Afghanistan that have cyber attack tools. Now, why would you suppose a terrorist would have any caring for cyber attack tools? Well, I just mentioned to you that cyber crime focuses on making money. Their ability to generate money to do the things that they plan on doing against us or any other nation is done, a lot of it, through cyber exploitation as well. This goes on on a recurring basis. Criminal organizations, whether it's, as I mentioned, the 3 categories there, also do drugs distribution, management, and so forth. They hide it, embed it in other files and that sort of thing, so that's [ Inaudible ].

The well-organized piece, I've got to tell you, when I was doing this many years ago, first of all, there was very little law that told me I couldn't do it, but I never, as a matter of fact, never hacked anybody that didn't deserve it. Actually, every time I did it I had authorization to do it. I worked for the Pentagon back then. I was in uniform working for the intelligence community. And it wasn't well organized. There were a couple groups up there that have been around for close to 20 years now. DefCon is one of them. Black [ Inaudible ] is another. These are groups of loosely connected individuals who have a grudge against Microsoft, maybe Apple, or maybe an organization, and they kind of team up, play capture the flag, and attack. Those groups generally don't do a whole lot of harm. They do a little bit of embarrassment. They'll deface web sites. They may substitute things that are on your web site, denial of service kind of stuff, perhaps. But generally those groups are not the ones--I do worry about them, but they're not the ones that cause me the most staying-up-at-night kind of events.

Today the groups that are attacking us are extremely well organized. It has long matured from those kids that we hear about to state-sponsored and resourced activities. There are a number of leading industrial nations in the world who have it in their economic strategy to actually use the internet to research R&D activities of an area perhaps they're interested in rather than stand up their own capabilities. And guess who the primary targets are when they go out for R&D information? Look at each other, because you are. And why is that? Because a lot of R&D goes on in universities and schools and colleges. A lot of grants are granted, everything from engine propulsion to cement construction to almost anything you can imagine. So why not go out and pick that stuff up. It's certainly easier and more cost effective to exploit it that way.

We had a number of years back a major breach in the United States involving the compromise of several supercomputers and [ Inaudible ] high-end computers at your schools. You know, no one really owns one of those things. It's kind of a lease-share program. The government may sponsor the framing and so forth, but it's shared and this university has so much time on it and so forth. Well, those supercomputers were hit. There was a little program called Moonlight Maze way back when. That was a secret cover name. It's in the press now. And the way they were successful at getting into those supercomputers and looking around was they attacked anything that had a .edu. Because remember, the creation of the internet was really for you all. It was for



START HERE  
GO FURTHER  
FEDERAL STUDENT AID®

universities to exchange information among universities, scientist to scientist speak, and very open, very collaborative information exchange. The internet has never really grown out of that approach. We talk open source. That's software collaboration, but protect the information. So you still remain a very active target in the targeting list if you have a .edu because I will tell you something, not to be insulting, but as a community, your security isn't really up to snuff. I'm sure that shocks you. The old way, as I mentioned, is just get in there, hit something, get out, make a big splash, you know, etc. Motivation back then was bragging rights. I would go to DefCon and I would hear someone brag about how they broke into somebody's industry because they didn't have this security feature and so forth. And the press would blow up that person. You may remember a lady by the name of [ Inaudible ]. She was a bored housewife in California, didn't have anything better to do during the day, so she teamed up with another hacker by the name of Dark Angel. She was in her forties, he was 16-something. But they connected, so they started attacking things out there simply because they were bored and recognition. They both talked about their exploits in Las Vegas at DefCon and they were both arrested afterwards. People out there doing that.

Well, the folks who are coming after us now aren't likely to show up at DefCon in Las Vegas and give a speech on how good they are. As a matter of fact, they're good enough that it takes us time at times to figure out they've even been in there. There is a major mortgage company, in fact, that was again in today's *USA Today*, that was compromised for over a year. The company didn't even know it. They discovered it last January, that for in excess of 12 months someone else owned them, and every credit card, every mortgage account, all the privacy information that was affiliated with those accounts now belongs overseas in a couple different countries. If you haven't gotten a letter from them, then you're okay. But if you have, you know who you are.

I mention intelligence. It's a little unusual for the government or a government rep to come out and talk about the intelligence community and things that are going on. But we think that it's important enough to share some of those things, so that's why I talk about the intelligence community initiatives and so forth. You may also remember on May 29 the President coming out and the White House launching the national cyber initiatives and talking about the things that needed to be done, how cyber security now is a major initiative of this administration, how it can impact not only our economic survival but our way of life. And I just want to take a few moments to like really make the point home here.

If you can think of any part of your life that sustains it or makes you happier or pursues your endeavor that is not computer controlled, I'd like to know what it is. We need computer control in our golf games. I'd bet you at the end of the day when you throw in your scores someone tallies them up in a database. I talk to 72 hours before chaos, and no one wants to live through chaos. You've seen some nations in the world that have gone through that. Let me tell you why I do that. How many hours do you think it takes to refuel a gas station? Hint: 72 hours. How much time does it take from placing an order out of a supermarket to refresh the shelves? How about 72 hours. How long does it take to get a fleet of trucks to move interstate commerce, tagged, ready to go?



**START HERE**  
**GO FURTHER**  
FEDERAL STUDENT AID®

About 72 hours. Our whole logistics survival now is based on just-in-time logistics. Just-in-time logistics means real reduction warehousing. So it's producer to retailer. That's about 72 hours. Imagine knocking out any of the critical infrastructures that support fuel, water, banking, health, food; because all of those things I mentioned are extremely connected in this country. We pride ourselves on technology we've gotten, how we've connected it, how we've made our lives better; but we've also painted ourselves in a bit of a corner, if you will, based on what the threat looks like today.

You may have heard in the paper about brownouts, electrical brownouts. You may have also heard some commentators say, gee, we think that maybe it's a cyber attack. Well, if you understand how electrical power is controlled, perhaps you understand how the flow of water is controlled. It's all valves, it's all switches. These things are controlled by items called SCADAs. SCADAs are RF-generated switches that open and shut things. They are also controlled through the internet. If you break into those, you can play with the SCADAs, shut off water coming from the Colorado River to Los Angeles, change the power grids around. Those are the things we worry about.

In the earlier days I did some [ Inaudible ] intelligence in my time--I'm a retired Army officer, started out as infantry, then intelligence, then the signal corps. During my intelligence piece, they actually paid me to run around looking like a bum, walking around to bars, to see what I could pick up in the area of operational security for military operations. If I ever got compromised and someone said I know you, you belong to 902nd MI, that was the end of my mission. I pack up my bags, I go home, because they can't replace me. Once I'm compromised, I'm gone.

So the days of having spies out there doing that kind of stuff are pretty much over with. However, if someone does the same thing using the internet, exploitation and attack, you never know who it is. You may find an IP and you may block that IP, but gee whiz, you know how easy it is to get another IP and do the same thing? So that's why this is much more profitable to do it this way.

ROI. I already talked about ROI in research and development. [ Inaudible ] beginning to wonder, just think about it, is there any connection possibly between the way the American shuttle aircraft looks and the Russian aircraft looks? Any possible link out there?

Motivation. The economic aspects are just phenomenal. If someone can bring down a financial critical infrastructure, you know what that means. If someone -- you don't know what that means?

**[AUDIENCE:]** [ Inaudible ].

**[LORANGER:]** Very good. You're keeping up on your current events. This is a whole new world of doctrine for military operations. Recent engagement between Russia and some of its satellite countries where they attacked using cyber attack. They cut off their services, denial of service for command and control, all that sort of thing, then they



moved in the tanks. It's much easier. That's happened in several other places on the grid today. Good point. Thank you. So political gain is also very important. We talk to that through our traveling folks.

Wireless is a good thing to probably mention right here. How many of you all have wireless systems? How many of you all have crypto on them? How many of you all use that crypto? Okay. The rest of you all are at risk. Just driving down the road between Baltimore, Maryland and Washington, D.C., we had one of our executive's cellular phone hijacked. That means it wasn't physically taken. He was driving down the road talking on it. It was exploited. His access code was taken. And we received a bill next with like \$15,000 of phone calls to South America. Your Blue Tooth. How many of you all use that? It's exploitable from a certain distance. So wireless is a very dangerous thing. Would you be concerned if I tell you that I can turn on a cell phone that's off? Okay. Didn't say I did. I said would you be interested. [ Inaudible ] You know, the cold war was really a scenario based on the last bullet. We outspent them. Quite frankly, we just outspent them. The last coffers that brought the Soviet Union down were based on Star Wars. Just outspent them. We can't do this with this threat, because it doesn't take a million-dollar computer to do this. The computers that are being sold over the Christmas holidays for \$197 can do the same thing here. It doesn't take a computer scientist to do these things anymore. When I was playing around with it, you at least had to understand what happens after the cursor. Today you don't. If you, picking on this lady right here, don't like that gentleman and you want to cause him a lot of problems, you can go to a web site, create a virus, and launch it to him in his e-mail. He will open it and his machine is hosed. By the way, that's free. If someone else in here wants to give someone else a bad time, there are a number of malware sites up there that let you create almost anything you want, and all you need to do is be able to spell. That's all you need to do. And have a "to" address, and it's sent. If you want to be more sophisticated than that, there are sites, illegal as they are, that say, hey, I will custom software develop for you. You just tell me the target and what you want to happen. Send your money. And by the way, it's an SSL site. They develop for you. And if you don't want to launch it, they'll launch it for you. That's all out there. So the days of having to understand how to write code, how to put it all together, are not necessary to be a hacker and menace today.

Just some trends here. As you're looking at the trends here, on your left you will see about events per day and then what we have to scroll down to -- I'm holding a seat up here for you, sir. The CIO from FSA. So you look at number of events and this continues to climb. Not every event is something we investigate. But just for grins, Department of Education, how many attacks do you think we get in a day? Give me a number, anybody. Ten? Any other number?

**[AUDIENCE:]** 10,000.

**[LORANGER:]** 10,000. Have you been in one of my presentations?

**[AUDIENCE:]** No, but I figured [ Inaudible ].



**[LORANGER:]** You're absolutely right. But the number is 10,000 per hour. Okay? That's what we look at almost every day. Now, if there is a holiday that's recognized around the world, the numbers go up because there are more people not engaged in work or school or whatever the case may be.

**[AUDIENCE:]** [ Inaudible ]

**[LORANGER:]** Maybe in this country. Maybe in this country. The next chart on your right represents what we see and what we actually have to investigate. So for the record, we investigate, through the use of automation, every event and every attack that comes knocking at our door, wherever it may be. Some are more interesting than others. We may get new scenarios, new fingerprints, new approaches, and then catalogue those. But those are tools. My buddy at National Security NDC tells me I can produce an absolutely secure system for you. I said bring it on. He said, but it won't have a power cord. If you can't plug it in and turn it on, it's pretty secure. But if you have to operate as we do when our customers are coming from everywhere, and we've got to make our systems available, at times we've got risks. So we do have a few breaches every now and then, and we learn from those and we protect them.

Bob will talk to you about some of the things that we're most concerned about in the department today, and we'll talk to you about some of the remediations. And it is things that we see as we exchange (we, you all and us) exchange traffic and connections. So it's a mutual shared risk or mutual shared threat that we're trying to remediate and address.

Another little cute term I want you to learn here. In the intelligence community, bad guys who are doing cyber things to us are called actors. Bad actors are what we worry about. We've talked about all these but, you know, we haven't really talked about this one right here. Used to be when I got in the business, I was really concerned about the bad guys outside the wire, to use a little military term, not people that were inside working with me. And that was a substantial amount of the threat that we had, bad guys on the outside trying to get in, trying to gain information, trying to become one of us, mimic us, whatever the case may be. But today the threat is fairly well balanced of both internal and external. Now, we can always recognize a friendly event when as soon as something happens to a network or to a system, we immediately get a call and say, gee, I didn't know if I pushed that button that was going to happen. We can recover from those. But there has been a lot of malice activity, from the studies, from people on the inside.

Had a case many years ago of an insider working in the ADP center. That gives you how long that was, right? Was shaving off the 100th cent off every insurance account and putting it into another account. He did that -- he was a team -- did that for over a year. Made themselves a pretty tidy sum. Their downfall, however, was they couldn't figure out how to get the money out of that account without cashing in a death policy. But nonetheless it's there.



START HERE  
GO FURTHER  
FEDERAL STUDENT AID®

We have had cases where employees who work on a system, especially HR systems or payroll systems, that say, hey, if I ever get fired, I want you to crash the system. And the way it reacts to if the name comes off the active payroll, it crashes the system. In today's world of temporary employees, if you will, very few employees out there now sign up to a company and stay there for 30 years. They move around, especially in the technology arena. It's not uncommon for departing technologists to leave an account active in his old company to go to a new company and drain that information as an advantage to his new company. So training issues, theft, malicious actions are all part of this. Wasn't a big concern many years ago, but now it is.

Now, as I mentioned earlier, the President made a speech on 29 May that talked to some of these things. There are a number of national-level cyber initiatives, and I think it's important when we talked earlier about sharing information between us, it's important that we establish a coalition between universities, colleges, so forth, and the department in sharing this kind of information. You need to be made aware of it. There are also things we can do collectively as we interface, collectively as we grant each other access and authorization. So we'll consider this a subset of the national initiatives, if you will, to improve security.

A couple things that we have done in the national security directives 54 and 23, those are directly related to the 12 cyber security initiatives I talked about and things we need to do. One of those, by the way, is education. Education of not only the awareness things we're doing here, but education of the next generation of cyber warriors, computer scientists, cyber defenders. We need to have that. You heard the Secretary talk on Monday about how we needed to get back to where we were as leaders in many areas. This is one of the areas we're not exactly the leader in.

OMB, Office of Management and Budget. We really pay attention to that office on the federal side because they are the folks that contain our budget; they drive our federal CIO activities and provide us a lot of guidance, and so forth. One of the things that they do is in the information assurance arena, the Trusted Internet Connection. Now, one of the problems that we were having across the federal space is we had a gazillion points of presence for internet. No one can defend and protect or harden a gazillion points of interest. No one can. So we've reduced those. For this department we're down to 4. We have a model department across the federal space, 4 internet presences. We can defend those. We can configure those. Something to take back to your colleges and universities.

We are very close with the law enforcement community. When you're in the cyber defend business, you have to be, because unauthorized penetrations, access, and so forth, that is generally the crime. And law enforcement guys pick that up and do the investigation. Our legal arm is our OIG.

The 2 major goals that we have in the initiatives are listed below. We absolutely want to stop critical vulnerabilities. I would love to as a cyber defender say we want to stop all



vulnerabilities, but that's not real. That's not real in the ability to do it and it's not real in the ability of how much money it takes either. But the critical vulnerabilities we want to stop, and Bob is going to talk to you about some of those. And we want to extend the protection. We call them predators, bad actors, whatever the case may be. They're here. It's real. What you hear in the news is pretty accurate.

How many of you all ever had your identity stolen? Three, four? Three times right here, three times, and all of them because of a security lapse or a breach inside a federal agency. If you've lived through that--well, if you haven't, talk to someone that has and you become instantly more concerned about how your privacy information is protected. And we are absolutely committed to protecting that privacy information in the Department of Education. That's why we have the program that we have.

Law enforcement, FBI. I have permanent FBI agents that support the Department of Education for exactly this kind of reason. It was not long ago where the criminals were doing very well because the law enforcement guys didn't have the tools and so forth. They have forensic laboratories now that match anything you can imagine. You all watch CSI on TV? That's not an exaggeration. They're that good. One of the major breaches we had in one of the departments I came from before I came to Education was disclosed because law enforcement busted an auto theft ring. That auto theft ring was stealing good VIN numbers, putting them on stolen cars, and shipping them overseas. And you go, what's that got to do with...? Well, that auto theft ring had been hacked by another bad actor, moved to another location in the country, and because of what they were doing with VIN numbers--can you guess what department is responsible for VIN numbers? Starts with a T. They took that exploit that the auto theft ring had done, exploited it more, and were able to collect all kinds of information out of that department. CSI came to me and said, here's a secretary's e-mail, you want to do something about that? That's how close the collaboration is between us.

So, 2008 was a bumper year, 2009 was even a greater year in compromise and so forth; 2010 is off to a great start. I kid you not. So we want to increase awareness. That's why we're doing this sharing of information. And we'll put some more programs similar to this with Bob and the CIO, because it's imperative that you at least at the unclassified level understand as much as we can possibly share with you, because we have mutual interests to do that.

Bob will pick it up from here. He's going to talk about some of the top vulnerabilities we have today. This is not conjecture; this is real. This is what's going on. So, Bob?

**[ROBERT INGWALSON]:** Ten thousand hits per hour, huh? Does that scare anybody in here? Yes, that scares me. It's after lunch. Everybody stand up. Go ahead. Okay, sit down. Great. Now, Phil just got done talking about a lot of threats out there, and they're in this country. There will probably be some in this room. They're all over the world. But for a threat to be effective they need motivation and they need vulnerabilities on your systems. What are some of the motivations out there at some of the schools



they participate with? We're not moving along until I hear a vulnerability. Okay, we got one.

[AUDIENCE:] [ Inaudible ]

[INGWALSON:] Yes, money. Absolutely. That's one of the motivating factors from all of our threats: money. And it might not be direct money, going in there and stealing that credit card. It might be.... Yes?

[AUDIENCE:] [ Inaudible ]

[INGWALSON:] That's a good point. We'll take that back with us. Thank you. But as we were saying, not only direct theft of money, but also people can steal data, steal PII, sell it on the market. There are a lot of things out there, a lot of motivation for the bad guys to go out there and try and hack into your systems. But they also have to have vulnerabilities on your systems. So that's the good news, because we can protect against those vulnerabilities, right? We can close them down. If there are no vulnerabilities, bad guy's not going to get in, right? Well, that's the good news. But the bad news is that there are a lot of vulnerabilities out there. F-Secure and McAfee have identified around 350,000 malicious pieces of code out there ready to be launched against any one of us. The National Vulnerability Database has identified 40,000 different program vulnerabilities on products that we implement on our systems. GAO has identified that hardly any of our systems have hardened configurations. They don't come out of the box that way. And about 70% of our web sites are vulnerable to attack. So there are a lot of vulnerabilities out there. And guess where you can go out and find information on those vulnerabilities on some of these web sites here that are identified? OWASP, the Open Web Application Security Project. All of these are free to you. We'll talk about them in a little bit more detail as we move on. National Vulnerability Database, it's a NIST database, National Institute of Standards and Technology is the ones that keep that going. SANS, they identify a top 20 list, and there are many others. But go ahead and use these URLs, access these at your leisure, please.

We looked at the OWASP top 10. This is what they are. Every one of these has been used by a bad guy to do bad things. However, we're not going to go over them all. Let's go over the top 3 and talk about those in a little more detail. Okay? Cross site scripting was the top vulnerability identified by OWASP. Why? It's so easy to, you know, take advantage of by the bad guy. There are internet sites out there that direct them exactly, tell them what to do and tell them what sites are vulnerable. Now, it may sound simple in its simplest form, what cross site scripting will do, but I tell you, it's complicated. There are a lot of different variations of cross site scripting. We could go on a semester about that. However, in its simplest form, let's say a bad guy goes out there and he finds a susceptible site, he injects some HTML code, he gets the resulting URL, puts it on a link or in an e-mail, the unsuspecting user clicks on it and they get what they thought they were getting because it's the actual site that they thought they were going into. However, it has an evil twist on it.



How do you prevent it? Well, you want to validate and encode user input. You want that to be automated through your application. Then once you've created your application and feel its secure, go ahead and run scans on it to inspect it to make sure it doesn't have any of those vulnerabilities still in there. There's a lot of scan software out there that would help you with that.

The second one on the list for OWASP was injection flaws; SQL injections are the main one we're concerned with. What are SQL injections? Where the cross site scripting was browser based, this is actually injecting commands, SQL commands, through input fields that will be run against your application. It can look at your data, take over your entire application or your system. Now, how do you fix that? Again, tight controls on user inputs, and you want to avoid dynamically generated SQL code because if you don't allow that, they're not going to be able to insert it into those fields. And like cross site scripting, you want to run scans against it before you put it into production.

Now, there have been a lot of cross site scripting vulnerabilities in the past and there are places that you wouldn't think would be susceptible to that, like the Army. They've had it. United Nations, they've been hacked that way. Anybody hear about 150 million records of information from debit and credit cards being stolen by 3 bad guys this summer, 2 guys from Russia and 1 guy from Florida? Yes. They used SQL injection to get that information. We've also had them at the Department. Let me read you something here. This came from the Director of Information Security before Phil took over that position. It's from Jerry Davis. "Bob, the Department experienced a web defacement this morning as a result of a SQL injection vulnerability. Right now I'm gathering information on the last time the boxes were scanned. You may want to consider having Federal Student Aid external facing servers scanned for the presence of SQL injection vulnerabilities if they have not been scanned in the past few weeks. Right now it appears the hackers are well known and have hit hundreds of sites." Hundreds of sites. Everything I'm hearing, I think probably SQL injection will be moved to No. 1 on OWASP before long.

Now, if SQL injection and cross site scripting were brothers and sisters, malicious file execution would be a close cousin, because it's also using dynamically generated application code to input malicious files or file names that will be executed when that application runs its processes. How do you prevent against it? Only allow for accepted, known, good files and file names when the application is collecting them. When I say accepted, known, good, you should have a listing of those in your application of what you're going to accept. Don't accept anything else. Don't try to filter against what you don't want because there are just too many variants out there. And PHP seems to have some commands in it for encoding these files, and you want to be able to disable those commands. Go to the OWASP web site and look at the listing of them, give it to your application developers and let them have it.

Oh, there's one thing I wanted to mention that's kind of important on the SQL injection. Once the 130 million records of credit card and debit card information were stolen, it created a high interest in the federal government, and within a day the United States



Secret Service and FBI had submitted an advisory and alert to the federal agencies identifying the vulnerabilities and telling them how to fix them. I have that in soft copy. I'm going to attach it to this briefing on the web site. So make sure that your software developers get ahold of that, because it has coding examples and everything else.

But there seems to be a common thread for the things that OWASP identified, and that common thread is dynamic code and user input. If you have web sites like that, make sure you take the appropriate precautions and make sure you run scans against them to ensure the vulnerabilities aren't there.

I'm going to kind of rush through these because we're kind of running out of time, so if you have a question along the way, please raise your hand and we'll hit it right there. Okay? Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** For all those that had stolen information from the 2 guys? We didn't deal with that. It was in the news. I believe they do have the information of who, the information that was stolen, identifying the individuals, and I believe the banks have notified them. So if you haven't been notified, you probably weren't one of them. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** I think that was a canned question. I think she knew the answer. Let's move on.

This is the SANS top 20 vulnerabilities. If you notice, they don't lay them out like the vulnerabilities in OWASP. What they do is they categorize them into 4 different major categories and then talk about the vulnerabilities against each of the subcategories. I'm not going to talk about it in detail here. I want you to go into the site. All these sites are free and available for your use, so do so. But when they do identify the vulnerabilities in SANS, they identify them with a CVE number, which is a common vulnerability and exposure number, and they get that number from the National Vulnerability Database. This is the first screen that you'll get when you go into the National Vulnerability Database, and although I said it was a NIST database, it's actually sponsored by the Department of Homeland Security, the US-CERT division.

There are a lot of things on this. Earlier I said that there were 40,000 vulnerabilities in this database, and if you look right here, it says 38,012. Why did I say 40,000? Anybody have an idea?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Yes, exactly. If you look right here, that's when I printed that screen, but right here it's saying there's an average update of 14 vulnerabilities per day. That's important, because if you run scans and find all the vulnerabilities and fix everything that



day, the next time those scans are updated with the new signatures and so forth, you're going to find more vulnerabilities, at least there's a good chance.

It has the FDCC checklists in here. This has created a SCAP or a protocol that they tie to all the different vulnerabilities, but we're not going to talk about that in detail. Instead, we're going to click on this right here where it says Vulnerability Search Engine and see what we would do if we had a product coming in we want to implement it in our systems, we want to make sure it was secure first. So you click on that. You could put in a keyword search. Here I put in Adobe, clicked on software flaws, and I get a choice between last 3 years and last 3 months. I pick last 3 years. And for Adobe I found 228 vulnerabilities. If I would have clicked last 3 months, it would have had something like 36. But that's like 36 new ones in the last 3 months.

And also within this tool, it identifies the version of Adobe that's affected. Adobe Flash Player before those version numbers, or between those version numbers, and the Adobe AIR with some other version numbers. Adobe versions that are outside of that aren't affected by this vulnerability. It tells the date that it was published and it gives a severity rating. This particular vulnerability had a severity rating of medium. Look at this one, high, 10.0. That's the highest it goes. When that vulnerability came out on 7/31, US-CERT called a conference with all the different federal agencies to discuss it, talk about remediations. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Okay. It would be a good target to go in there and try to maybe take out some of that, but the bad guys don't really care about doing any damage to this database. They like this database. They like to go in there and find out where the vulnerabilities are just like you do. They want to find out so they can attack you. We want to find out so we can protect ourselves. Right?

Let's move on to some other vulnerabilities. Something like code mistakes, untrained users, and insecure configuration settings. First we'll talk about code mistakes. Code mistakes in your applications can cause a lot of heartache and problems. I think probably the largest breach that I've witnessed at Federal Student Aid in the last 15 years since I've been here has been a simple single line of code that once it was implemented, students started calling in when they were accessing that particular application saying, hey, I'm seeing somebody else's data. Well, immediately we shut down the site, but before we were able to shut down the site, there were 30,000 records of information that were compromised. Now, that made the news. It also had us answering congressional inquiries. It caused us to shut down the site for 9 days, required many hours of analysis and discussion, created bad press for the department. Allowed borrowers' identities to be compromised. Created late borrower payments, affecting their payment status. Increased call center activities. Required letters to be sent to borrowers explaining the problem. Required us to post messages on the web site, and required us to offer credit monitoring for those affected for up to a year. I'd say



that one line of code had quite an impact. So you want to make sure that all your code is tested thoroughly and use all the tools that are available for you to do that.

Untrained users. I think that's a no-brainer. If you have untrained users, it's going to be a security risk. Simple things like don't walk away from your computer while it's on. Don't send sensitive information over an e-mail unencrypted. Don't push that button. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Right, especially if you have sensitive information on it, then somebody might be looking in.

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Good point, good point, especially for those systems like over at the FBI. So what do we want to do? We want to provide training to the users. You want to give them initial training; provide them a general security awareness. You want to give users that deal more with security more in-depth training on the roles that they have. Take, for instance, the individuals that are creating that code. They need to be trained and aware of the vulnerabilities that we've already talked about. You want them to sign rules of behavior, not only so that they know what they can do, but also so that you know that they know what they can and cannot do. And then once they've had the initial training, you want to ensure that they have annual refresher training, because new things come about all the time.

Insecure configurations. Like I said, GAO says that our systems are not hardened. Well, NIST has a requirement by law to provide the standards or the guidelines for us to implement. What they have created is what they call STIGs, which are security technical implementation guides, and they have those for most of the platforms out there, so when you create your systems and you go through the builds, make sure that you use those types of configuration standards. During system upgrades, make sure that those configurations haven't been erased and that they're still secure. Then run vulnerability scans on those platforms and systems to make sure that the standards are in place. I should mention, up here I say vs. business needs. If you implemented all the standards exactly the way they're set, guess what? Your systems might not run. That's another problem that we have to overcome. So you have to weigh the risks of not implementing a particular standard with the risks of your business.

Now I want to talk about some special-interest items. I call them special-interest items because about 3 years ago we started getting these files from US-CERT that identified where individuals had downloaded malicious malware onto their machines and all of a sudden that malware was capturing information and sending it to a BOTNET source, and actually some of that information was coming from some of your computers and students' computers. How is it done? Through keyloggers. That's one way. Actually when US-CERT first started giving us this information, we thought all of them were



keylogger-type information. Does anybody know what a keylogger is? What's a keylogger?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Exactly. So as you're logging in, it's capturing all that information every time you hit a different keystroke, so it can find your passwords, it can find PII, everything else, right? But the vulnerability isn't on our system. It's on the client's system. However, we have a concern about it, because what it's doing, it's opening up our system if they learn those passwords.

What can we do? Train users. Train them so that they are aware of the situation and let them know what they can do: Implement anti-virus, anti-spyware, make sure it's current, all the patches and versions are current; implement firewalls to look at outbound traffic, make sure if there's any keylogger information leaving their computers, they're aware of it. Automatic form-filler programs. Has anybody been on the internet and they're putting in their user ID and password and all of a sudden a form pops down? Yes. Well, that's a form-filler password. It's so you don't have to enter those keystrokes next time. It's a security measure. Cut and paste if you don't have the form filler. This is what I do. I use a spreadsheet. I have all my user IDs and passwords on it, and when I want to go in and enter into a particular application, I copy and paste from my spreadsheet into the login. That way I didn't use the keystrokes, right?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Well, it depends on what that cookie is capturing. Yes. I am against capturing any type of sensitive information in that cookie. I'm against especially capturing it on a persistent cookie that's going to keep that information and it's susceptible to attack at a later time. As a matter of fact, it's --

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Right. I know. And federal regulation and Department of Education do not allow persistent cookies on their applications. We have one application that has a persistent cookie. I'm not going to tell you what it is. Okay? But it's been authorized by the Secretary of Education. And anytime we want to use a persistent cookie, we need it authorized by the Secretary of Education.

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Yes. Get back with me, will you? Okay. Let's move on because -- did you get his name?

**[SPEAKER:]** I've got his name.



**[INGWALSON:]** Okay. One-time passwords and Smartcards are 2-factor authentication if you use it along with your passwords and user IDs. What does it do? It keeps you from getting in there, even if the keystrokes are caught, they're not going to catch this, they're not going to catch that 2-factor authentication. Although they might capture the one-time password the first time, next time you go in, you have to use a different password, so they won't know what it is. So that's a successful measure to prevent them from learning your credentials. However, what it doesn't do, along with the virtual keyboards which we're going to talk about in a minute, is what it doesn't do, it doesn't protect the information after you're in. So if you're typing in sensitive information into the application, a keylogger can still pick that up. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Two-factor authentication?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Absolutely. That's a problem if people lose their...and that's where the one-time passwords come on, something like that, a token of that nature. And if they lose it, that's an administrative nightmare, isn't it? It's tough. And Phil's going to make a comment, because they're implementing some of this at the Department.

**[LORANGER:]** [ Inaudible ] So in the world of authentication [ Inaudible ], something you have, something you'll use, something you know is a PIN or a password, is something you are. I've seen various successful application of something you know, something you are, which is biometrics. So a template read off a finger, facial recognition, something of this nature, is very hard to duplicate. In fact, I don't know that it can be, not with technology that we have today. So that's the other 2 factors [ Inaudible ].

**[AUDIENCE:]** [ Inaudible ]

**[LORANGER:]** For the higher-end – your question was why is it not being used [ Inaudible ] because of cost. The short answer is yes. But the most common one, which is template reading or fingerprint reading, [ Inaudible ] is down to like [ Inaudible ] 895, 1995 a sensor, so that's coming down as well.

**[INGWALSON:]** Yes. I know a place that did the fingerprint reading, everybody was running around with only 3 fingers on each hand. I don't know what happened. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Contact lists?

**[AUDIENCE:]** [ Inaudible ]



**[INGWALSON:]** Yes. Don't go with that. As a matter of fact, come talk to us after this presentation. Okay? Let's go on and talk about the virtual keyboard. Yes?

**[AUDIENCE:]** [ Inaudible ]

**[INGWALSON:]** Well, I tell you what. We can't recommend any particular brands because that's the way the federal government works. However, the Department is using McAfee. Yes. Okay. But there are a lot of good anti-virus, anti-spyware programs out there and a lot of them are comparable. What I should mention, though, is that when you run those anti-virus and anti-spyware scans, you might want to do it from safe mode because what we're coming up with next after this slide is a program that will escape it sometimes when it's run on your regular computer.

We've already implemented the virtual keyboard at Federal Student Aid for some of our applications, not all of them. But it prevents keyloggers from capturing information. What you do instead of hitting the keypad is you hit the cursor on one of these virtual keyboard characters, and then it will populate into the login. What are some of the benefits or some of the ease of use for that? It's highly effective in evading keylogging. Yes, I just talked about it. It says true keylogging. I'm going to talk about that in a minute. Widely used by many financial institutions. If you go out there, at some of your banks you'll see this. Low-cost technology to deploy. Goes along with the next bullet. Your clients don't have to implement it on their machines. It's on the application. They pick it up. It can work in conjunction with the existing keyboard. However, if I was to implement it, I'd implement it and require its use for login and then turn it over to the regular keyboard once you get into the application. Keys can be entered by a mouse click, or if you just hover that mouse over one of those characters for 2 seconds, it will automatically populate. And the virtual keyboard randomly shifts on the screen. Why might it randomly shift on the screen? Because the bad guys can read that cursor position and figure things out sometimes, so it's preventing the reading of the cursor position.

So that's a pretty good tool to decrease the vulnerability of key logging. However, WSNPOEM is another animal and the virtual keyboard does not protect against it. Why? Because information in your browser is sent to the malware and sent out before it goes out, before it even is...if you have a little lock on your computer, a lock down in the screen where it says it is going to be encrypted, it is sent out before it is even encrypted. If you will notice what some of the variant names are for this, Banker, Banker...what do you think they are after? Yeah, they are after money. So, if you have downloaded this on your home computer and you are accessing Federal Student Aid information, you are putting us at risk. If you have downloaded it on your school computer and you are accessing Federal Student Aid information, you are putting us at risk because it has captured your user ID and password, and they can log in as you and do the same things on our systems that you might have been able to do. Also, if you have it on your home computer, it is not just affecting us, it is also affecting you and if you do online banking, you can bet you have some worries there. As I mentioned earlier, what do we do?



## START HERE GO FURTHER

### FEDERAL STUDENT AID®

Here are some impacts: Twenty-two thousand unique compromised SSNs since we started getting this information, and over 300 unique compromised user IDs and passwords. We have taken action on every one of those. Here it shows that the WSNPOEM is the main culprit for all of our compromises coming from US-CERT.

Again, what can be done on the application side? Implement two-factor authentication. Virtual keyboards, URL coding, header encryption, anything else...that does not help. SSL doesn't help. So, two-factor authentication and training and awareness – letting your users know what they need to do.

What can be done on the client side? Again, two-factor authentication, along with the application side. Keep patches and versions current, that is the most important thing, and run those scans – run them from safe mode. Does anybody know what I am talking about when I am saying run scans from safe mode? I see a lot of nods. You run it normally when you are in your normal Windows configuration, open to the internet. Sometimes it does not pick these up. If you go to safe mode, and you do that by reinitializing your machine, start hitting F8, all of a sudden it will pop up and ask you what mode you want to go into – say “safe mode” – you will pull it up, then run your scans.

These are the things that we do. When we find that, we immediately revoke the access for those users. And we have had to actually shut down some schools' access to some of our applications because of this until they have cleaned their machines and proven to us that they have cleaned them. So, it could affect you also. Has anyone in here been affected and we have contacted you and had you prove to us that you have cleaned your machines? You 5 in the back, okay. Immediately once we find this out, we notify the user and the school. We review the logs to make sure no suspicious activity has occurred, we look at IP addresses. If the IP address from the initial compromise was your school in Connecticut and all of a sudden we start seeing IP addresses accessing the same data from California, then we look further to see what was compromised. Then, we assist the users and the schools clean their computers.

So, I guess that is all kind of scary but it also shows you some of the things you need to do to make sure it is not affecting you. But we need to implement our security based on cost vs. risk, right? We kind of talked about that earlier, especially with the configuration settings. Threat times the vulnerability equals risk. Cost of implementing controls vs. the cost of not implementing the controls. I have heard some statistics that a breach in PII costs on an average of anywhere from \$90 to \$300 per record. That was a For ISSA research result a couple of years ago. Just recently, I heard the average was about \$220 per record. What if you had a breach of 100,000 records? Do the math. How much cost do you want to put into your controls?

Do you have any questions? Thank you all for coming today.