An Interview with

ROBERT E. JOHNSTON

OH 431

Conducted by Jeffrey R. Yost

on

28 October 2013

Computer Security History Project

Windsor, Connecticut

Charles Babbage Institute
Center for the History of Information Technology
University of Minnesota, Minneapolis

Robert E. Johnston Interview

28 October 2013

Oral History 431

Abstract

This interview with computer security pioneer Robert Johnston stands out for its documentation of early efforts to implement computer security systems and policies within corporations. Specifically it details his leadership with computer security in the insurance industry (at Travelers, The Hartford, and Phoenix Mutual) in the 1970s and 1980s, as well as his role as workshops chair for the Computer Security Institute, an important, independent, user-focused organization for inter-firm sharing of information and knowledge on computer security. He also discusses a secure facility (unprecedented within industry) he designed and oversaw that was used in discovery with the IBM-Fujitsu legal battle, and professionalization issues in the computer security field.

This material is based upon work supported by the National Science Foundation under Grant No. 1116862, "Building an Infrastructure for Computer Security History."

Yost: My name is Jeffrey Yost, from the Charles Babbage Institute at the University of Minnesota. This is an oral history interview that's part of our NSF-sponsored project "Building an Infrastructure for Computer Security History." I'm at a motel in Windsor, Connecticut. It's Monday, October 28, 2013. I'm here with Robert Johnston, Bob can you begin with some very basic biographical questions. Can you tell me where and when you were born?

Johnston: Certainly. New Haven, Connecticut, October 28, 1939.

Yost: I'd like to wish you a happy birthday.

Johnston: Thank you.

Yost: And did you grow up there as well?

Johnston: No. I grew up in East Hartford.

Yost: Who were your greatest influences growing up?

Johnston: Without any question, both my parents. I look back at many of the things; the traits I have and the way I do things, and I attribute these to either one or both of my parents. In particular, the one for what I call responsibility, was ingrained in me by my father when I was about nine or 10, and I said I need a bigger allowance. He said go find

yourself a job; that's all the allowance you're getting. I started delivering newspapers and delivered newspapers until I was 16, with some breaks because I worked tobacco during the summer. My mother told me after my father passed away, that my father was very disappointed when I started making more money per week working on tobacco than he did as a long term letter carrier. [Laughs.] He taught me.

Yost: Were there particular subjects in middle school or high school that were of great interest to you or that you had a special aptitude for?

Johnston: Science, primarily. I loved all the science courses. I'll say history; U.S. history was very interesting to me. I hated ancient history. Somehow, at that time of my life, it didn't seem relevant. In high school I got very interested in retailing, and the school had a retailing program and it had its own store. So I took the retailing courses, so obviously they were electives. I was on a college course program so those were extra courses rather than the primary courses you had to take. Loved it, so when I turned 16, I started working at G. Fox and Company, very well known retailer. Enjoyed it very much. The other thing that I loved the most and I was noted for in high school is photography. I had started that before I got into high school. So I got a job in a camera department. You want to talk about somebody in the reign of luxury, able to take pictures whenever he wanted and all that sort of thing; all these great cameras. Just before I started college, the summer before I started college, I got promoted to assistant manager, which was practically unheard of for my age; I was 17. You had to be a manager in order to open the camera department because it's under lock and key from end to end. In fact, neither the manager nor I had

the key to the doors to the department. We had to go to a floor manager. They were making sure who was going to be present. We had keys to the internal locked up supply room, and that sort of thing, that was fascinating. To give you an idea of how great a store G. Fox was, I went into the service in September 1959, in January I received a check for the sales that were made between September and December because they kept an open book for me and when people asked for me, they put the sales in that book, and I got this check out of nowhere. And again for the next two years. It was just that kind of a store. I thought I would go into retailing. Went into college. Quite frankly, felt they weren't teaching me quite what I needed to know.

Yost: And what year was this and what school?

Johnston: This is the University of Connecticut. First year I was a freshman, I decided halfway through the year I'm not going for another year. It certainly wasn't due to the fact that it was costing me money. My parents couldn't afford to send me to college; I was paying for it because I was working. But I said I don't see any benefit to this, I said, I'm quite successful in retail already, I love photography, and this was still a draft year. I said if I stepped out of college, I'm going to get drafted. I'll go into the service and I'll be a photographer. I signed up for the courses and all that good stuff, and that sort of thing. Guess what? Course got cancelled. Now what do you do? Wait around? Do you go back to school so that you don't get drafted; continue working? I said aw, I'll go in; I'll make it anyways. Well, because I had ROTC, through all the trainings, I was a platoon sergeant so I never did any KP, that sort of thing. I was going directly overseas and that was

several weeks away so they found out I knew how to type — and I'm a good typist — so I got to work in the orderly room; again, no KP or anything else. Usually when you're holdovers, that's when you get all the messy jobs. They always tell you don't volunteer for anything, well, when I got off the truck at the base that I went to in Nuremburg, Germany, the first question was who knows how to type? I became a personnel clerk and then the personnel sergeant. I'm industrious; I worked hard. I worked on some very classified assignments not at my station. I had a high crypto clearance, and the reason for that is — why does he have a high crypto clearance, he's a personnel guy — simply that we had to encrypt status reports for the battalion I was in. I had the necessary level of clearance without the crypto, so they gave me the crypto clearance, and that was one of those extra duties, encrypting messages every day. There were no electronics to do this, this was all done manually. [Laughs.] Open another page in a code book and use it. You don't stay on that very long if people can't read your encrypted messages after they decrypt them. And again, that end was that way. Anyway, I went on several classified assignments as a result of that. You get that combination of this guy knows how to type, he's an effective manager, and he's got the clearance. Everybody says, jeez, you were just in personnel. It was really quite different. Then came back to the States, Fort Gordon, Georgia, talked to my wife; we came back in, let's see; came back in December 1963.

Yost: You had gone into the service in 1958?

Johnston: Correct. After about a year — came back from Germany in December 1963, must have been 1965 — oh, I know what happened; that triggered it. I was assigned as a

personnel sergeant to guide career personnel into desirable career fields. It sounds like a recruiter; no, I wasn't a recruiter. I was in the personnel department. We used to look for the people that had the right scores and that sort of thing; so I was a guidance counselor, effectively. At the same time, we were just implementing computers at Fort Gordon. Most of our stuff was coming down. Anyways, Vietnam was just starting up and I got to be the designee — which I hated — to select the people to go. Computerization wasn't there at the time. I came home one day and said to my wife, you know, I need to change career fields. This is not what I want to be. What am I gonna be when I get out, if we stay until retirement. She said fine, what do you have in mind? I said I've got two courses as possibilities and you're going to decide. One was computing, which meant I'd be away for three months, never home; and the other one was aviation equipment repair, which meant I'd always be stuck at an airport to do it. Both very highly rated in the private sector, both well paying jobs at that time. I said it's your call. She said well what do you think is better? I think computing is better because we can get a better choice of where we can live; I'll get to meet more people in different aspects. I'm a broad minded person. She said you go, I'll manage the kids. She got a deal. So I went and took the computer course. That's what launched me into [pause]

Yost: That's the programming school in 1966.

Johnston: That's correct.

Yost: So that's a three-month program. And where was that?

Johnston: That was up in Ft. Monmouth, New Jersey. The interesting part of it — a little aside about the course — to be specific, it was 17 weeks and we had two college professors monitoring the course. Their report was what's been taught here in 17 weeks will require a four-year program at a college. I mean, they really crammed material into the course, but I loved it. I mean, just had a blast at it!

Yost: This was full day of instruction every day, and study at night.

Johnston: That's right; lots of homework. [Laughs.] Guess what, I was platoon sergeant for the whole barracks there, and my assistant platoon sergeant was also in the course. You became specialists when you became programmers. In those days, specialists weren't highly regarded; eh, techies, what do they know? The day we got the orders converting us to specialists we were damn proud of it; had it sewn on our sleeves. We're walking from the seamstress back to the base, to the barracks, and the captain drives by, stops in the middle of the street and says who did this to you? We explained it to him and he said okay, that's what you wanted? We said yes sir. He said okay, you two still run the doggone company drills until you go. Yes sir. I'll tell you, the Marines looked at us; I had a platoon of Marines in that barracks and they looked at us like what the hell are we listening to? [Laughs.] Then I got the orders.

Yost: Can you describe the type of instruction you received, were there certain languages you were taught?

Johnston: Primarily there were two. One was a generational machine language; I can't even remember the name of the computer it was on. It was only to teach us how to do UNIX code rather than COBOL, so that you had two basic sets of skills. One was . . .

[INTERRUPTION]

. . . so you had the ability to hit a coding sheet and write in machine language, rather than just COBOL. That really proved to the most beneficial of the training, as far as I'm concerned, because that's where I learned how to do the sort of work I did on the IBM systems. Even though there was no training for IBM computers, it was meant to be a general training so that whatever computers you got on you could transform, which I did. I enjoyed the duty there. My wife enjoyed it. Obviously, we lived in base housing, which wasn't where the computer station was but it wasn't that far away, and we had a good time there. I was offered a guaranteed assignment to Hawaii; a very good job; more than likely I'd have gotten promoted kinda quickly. And I did get promoted. When I became a programmer I was a Spec 6; and I was promoted to Spec 7. There were no higher specialists; I would have had to go to master sergeant, which would've happened if I had taken Hawaii. My father had a heart attack while I was there and I'd gone home to see him. I talked with my wife; we had planned to stay in the service, it seemed like a good row to hoe. My biggest frustration was twice there were openings for warrant officers; I wasn't chosen. I looked at my wife and said you know, it's time to go home. My father wasn't doing that well. I'll make you a deal. I've got 90 days to reenlist at the same rank. We'll go home; we'll live with my parents; they've got the space for us; I'll get a job that makes at least what we expect to get as a minimum, which we set above my military pay

because things aren't quite as cushy on the outside. Came home, made up a resume, went to a hiring agency, got three interviews, and within three weeks I had three offers all above our minimum. So that it made it real easy. We had saved money; we went and got an apartment, etcetera, and settled down in East Hartford again. And I was working at the Travelers for the next 10 years.

Yost: Before you made that decision, took that job, you were a manager of personnel processes relative to information security for the army. Was that in logistics?

Johnston: That was in logistics, yes.

Yost: Can you describe that for me?

Johnston: The computers were all dedicated to one thing, and that was identifying stock, where it is, so that other people have a pick list and could pick it up. The problem was that almost everything was managed by procedures, written procedures. And what had happened was, by error, 67 boxes of paper were printed with the entire atomic bomb inventory on the island of Okinawa. Data Center was told to dispose of it; they provided it to the disposal agency, but did not prescribe that it needed to be destroyed. The agency turned around — you know, the beautiful large printer paper — turned around and sold it to various venders on the island and they used it to wrap. [Laughs.] Paper was expensive in those days and this was a lot cheaper. One of the officers, or his wife bought something down in the Naha, Okinawa district area, thought this was kind of strange, and

then it hit the fan, let me tell you. We policed up all we could, it was a big effort. I just went up to the data center manager and said look, you've got to have procedures in place. Do you? He said no. I said fine, I'll get the clearance to write them for you. As soon as I wrote the first set of operations procedures — I mean everything was hand script; I typed, so they could read mine, it wasn't scribbled notes — and he liked it so much and word got around. So finally they said Specialist Johnston, you're going to write the procedures for programming, etcetera, etcetera, etcetera; relative to keeping this secure. To give you an idea of how well I was regarded, due to change in organization in 1967, where logistics officers from the other branches of service were to come right into the programming area and learn how things are done so that they could take advantage of it as well, or possibly implement them. It was a team of us. I had an army captain; I had a marine corps major, and a navy commander who sat at a table set up for four people. I was in charge, which again, is virtually unheard of, especially in those days. In the beginning it was, eh, what are we doing listening to this guy? Very quickly they found out, here's a report, here's a report, they can't read the reports, they don't understand why it was done this way and I had the knowledge. So that's when they learned why I was in charge and was making reports on how they were doing. So it was a challenge. Career wise for me, having responsibility and executing it is what's so important and it has been all my life. Again, that word "responsibility" comes across from when I was a kid. And that's what I'm doing today, after all.

Yost: In the late 1960s, were the computer systems batch; was it a batch operation? Was there any time sharing?

Johnston: No time sharing. Everything we did; the only time I touched a console was when we had a hung system and they wanted to find out if there was some way I could get it running, even if I was to patch memory. The rest of the time, just by hard, fast rules, programmers don't get near consoles. A little aside to that is we had an extra computer — well, it's not an extra computer, it was a dedicated computer — outside of operations. And when I was working nights, that computer would be off because it was only running during the day and I got to play with it. It was a very thrilling time for me. Like I said, the big thing for me was the fact that troubles at home; oh, there was one other thing that went into my decision for getting out; I was watching the newspaper ads for programmers and slowly but surely over those three years — I knew that I had to make a decision in those three years because that's when my enlistment was up — I watched them say degree required, degree required, degree required. Oh, here you go; you better jump ship while you can still make a name for yourself without a degree.

Yost: A short while back I did a short term historical research project on a system for the Air Force logistics operation, the Advance Logistics System that CDC served as the primary hardware and software contractor. You mentioned that the other branches were coming to the army to learn from you. Can you talk a little bit about where the Air Force and Navy were at skill-wise and knowledge-wise, with regard to information security and logistics at that time?

Johnston: Almost non-existent. Anytime you started to talk about security, they'd say well, that isn't necessary because nobody understand anything except those guys that work on them. And then I said well, maybe you don't have to secure the programs and the code, but you've got to think about backup and recovery. They said we have a power generator. I said, yeah, and what happens if you lose the data? Where are your alternative copies? Oh, we don't keep those. So you sort of get that, because that's the first step in security, anyways. Then I tell them the story of the mistake in dumping the printouts. Since all of the nuclear was in the possession of the Air Force, we had the master inventory but they had the storage facility. Suddenly they said, yeah, you're right, we have procedural controls to make sure that information that we're printing doesn't go where it doesn't belong. So I guess, at least for the bases on Okinawa, it sort of got ingrained. Almost anybody can do procedural work, you don't need to have a degree in computers or anything else; you just have to use good logic. At their request, I visited the Navy's computer facility down in Naha, Okinawa. They said all we want are your observations. Don't say anything here; bring it back; write it up; we'll consider it. To me, it was a horror show. Just before I was ready to leave; that was 1967, I was leaving in 1969; just before I was ready to leave, they said would you mind coming back and taking another look. It was like night and day. What happened was that the person responsible for the Data Center had actually wanted to do these things but couldn't justify it. Now it gets an outsider who's recognized elsewhere for doing good security work, the report that I gave to the Navy commander went right to the commander of the base and he said do it. The data center manager was real happy about it and he didn't waste any time getting it done.

Yost: Were electronic emanations a concern; was there tempest equipment in use at that time?

Johnston: No, not at all.

Yost: Policy. . . or procedural standards, so that mistakes aren't made in letting secure information out?

Johnston: That, and physical security of the data center.

Yost: And when you left active service to start college in 1969, I understand you had a choice between going to; or fairly early on, while you were there, you had a choice between being a database manager and a security manager. Can you talk about that decision?

Johnston: That decision was real easy. Databases, at that particular time, were narrowly constructed and essentially your only contact in the business department was your counterpart. After all, you're a techie, what are you going to do, talk to a line manager about this database? No, you're going to talk to your contact. That's not my idea of fun. I said well, the security manager's going to have all aspects; he's going to get to talk to people in all departments. I was in the commercial line systems division, so there are several departments, obviously, operating off of that. Plus, I'm going to have to deal with

the data center, and training; I had interface with almost all areas of the company. Ted was a good guy; he just didn't think forward and I knew he wasn't going to get promoted; and like I said, he got canned after I left. I don't know whether I was carrying him without being aware of it or not.

Yost: Travelers was really starting computer security infrastructure at that time, then?

Johnston: That, and I think as much as anything that created that fervor, they were the first company to have a national database that was accessible from all their agencies, independent agencies; and that was a real time system. I think that's where the paranoia started to come in that it's not just that little room over there. The data center was; imagine a two-acre building but one story, that's why it covered two acres. You don't have to just secure that place, and that was well secured on day one, I must admit that. But, that's really what started the whole thing was when they realized that this data was flowing all over the country. That was the awakening of the necessity of a lot of the different processes.

Yost: At the end of the 1960s, Willis Ware led a Defense Science Board committee that looked at changing concerns and realities of security with the advent of time sharing systems, and it was focused on military security, but I think it was some years before that became a public report. He wanted it public from the start because he wanted to influence industry. I was wondering if you knew about that at the time and either that work of Ware or some other emerging work in either the military — Roger Schell was

just starting research program for the Air Force — or the academic community — Peter Denning, Jerome Saltzer, and some others had done some work. Was that influencing practice in industry at all yet?

Johnston: Not that much, unfortunately. Those that looked at them saw them as too narrowly defined; they weren't comprehensive enough. That was the nature of the trade at the time; everybody was working in isolated areas or protected areas at the time. That's one of the things that caused me, after I became security manager at the Travelers, I suddenly realized there wasn't any useful information coming out in the trade press. It was virtually sterile. I can recall trying to preserve the few that there were. In my first effort, there was only six or seven articles in an entire year across the trade press. This has just got to change. I wasn't ready to write, yet — first of all, they'd say who the hell is he? — and CSI, Computer Security Institute, pioneered by John O'Meara , when that came on board; I immediately went to my manager and said I've got to go to that conference. That was probably 1973. I went to the conference; he had 12 workshops; and I'm sorry John, but they were all terrible. I didn't get to go to all 12 of them. The presentations were — the whole audience — were good, but not the workshops. I contacted John and I said John, you're not running good workshops. He came back and said Bob, would you like to be workshop chairman? Find a way; if you do I'll pay your way to the conference. I said yes, but you've got to understand, I'm going to give one or two workshops, too. He said that'll be fine. I said what do you think about doubling the number of workshops to 24? He said if you can come up with 24 good courses, by all means. And that required a lot of personal time and effort. First of all, you've got to

understand what I was gathering in the way of information and reviewing these guys to see if I was even going to let them get up there and talk. So I was learning different perspectives constantly and it was a joyous time for me. I wrote several papers, too, for them but they came out with the *Computer Security Journal* and I wrote three rather significant papers for the Computer *Security Journal* over three years. I was researching the various security products. I did one on the mainframe products. Venders weren't even going to answer your questionnaire until they realized the publication that it was going in. And then I did one on CICS products; software that supported CICS, which was a maverick at that time. Best that there was, but it still was a maverick. And then a year later, the world had; the mainframe security world had transformed itself quite a bit in three years and so I redid that paper again. Of course, at that time, I was still writing RACF, that was the best of choice by the Travelers. And I was seeing the other products; in fact, I went to the training conference for Top Secret, and a couple of others, so I was noticing what was missing with RACF. So I redid that paper again to — well, I wasn't trying to beat up IBM — I was trying to get them to put the features in that I thought were necessary. And I think it did influence them quite a bit when they were taking a look and saying wait a minute now, when you look side by side, we don't look that good.

Yost: Can you tell me what you know of John O'Meara's background and do you know what led him to found the Institute?

Johnston: He's an entrepreneurial-type guy and real good at organization. He knew he had some basic education in computers. He was in his; I'm going to say perhaps not more

than 30 when he founded the Computer Security Institute. And it was his knowledge of computers, and seeing where it was going, and seeing that this was a product that would sell.

Yost: Was he with a company or had he been with [pause]

Johnston: I really don't know his employment history prior.

Yost: Okay. But this was a full time job, once he started.

Johnston: Absolutely. He had one floor of a building for his staff. I could probably get you contact information for John. I just have a sneaking suspicion I can dig something up. He doesn't answer everybody anymore, because people still try to get back to him, but I think he'd answer me.

Yost: You mentioned RACF. When you came to Travelers, was it entirely using IBM at that time?

Johnston: IBM in-house, so to speak. You want something, go to IBM and get it; master contract and all that sort of thing. When I went to the Hartford Insurance Group, they still didn't have a mainframe security system. So that's when I told them we're going to put in Top Secret and we were really thrilled to pieces with it. This is during the transition at The Hartford, which is little more than a year. My first job was to come up with a

computer security policy for the corporation. They had been trying for five years and had never been able to get everybody to agree. A friend of mine — he was my next door neighbor when I was growing up — was an executive in one of the departments. I called him up; hello Bob, how are you, and all that kind of thing. I said, can you tell me what the heck is going on with the rejection of a master computer security policy for the corporation? He said, well, I will give it to you from my perspective. Whoever is writing this thing doesn't realize the make-work that they're creating, without showing what the benefits, if any, are. And that's what you gotta do. You've gotta make sure you're limiting the amount of work you're creating and you're showing tangible benefit for what you prescribe. Probably best piece of input I ever had, because it only took me six months. When I sent the first draft, now wait a minute, we haven't seen this before. I said no, it's a brand new one; I wrote it. And of course, here I am with the company about three months when this goes out and I notice [people saying] oh, what does he know about anything around here? If you follow me. But it only took me six months before it was signed by the president and presented to all officers of the company in the auditorium, saying, you're gonna live by this now. I made a couple of presentations on that because it was the only known corporate computer security policy in the country; at least, none were published yet. So that got me some notoriety as well.

Yost: Did you have any involvement with IBM SHARE in the 1970s?

Johnston: No, none whatsoever.

Yost: I interviewed Eldon Worley and Barry Schrager, and Worley did some underlying research within IBM Research for RACF. When it was really developed into a product, he was just an advisor, but much of the underlying structure and code began with his work. And then Barry Schrager developed ACF2. Did you try and influence, as a customer, IBM early on with feedback on RACF? First of all, was that the first security product that Travelers acquired and implemented?

Johnston: Yes, it was the first; and it was implemented about two years after I became the departmental computer security manager. They did a really good job.

Yost: That would've been when it came out in 1976?

Johnston: Yes. They did a really good job with it. I heard the horror stories at other companies where they weren't careful in their analysis in installing it, and brought the data center to its knees, etcetera. Biggest frustration we had was with staff members who didn't like the logon passwords and having to change them, that sort of thing. That, and I quickly implemented a violations tracking so that I could find where the problems were and get some training into those areas. Some people weren't all that happy that security was able to see who was having a problem. Some of my analysis was quite interesting, but that's so long ago, let's leave that behind. Yes, some of the people wound up with extra training and a few people got duties changed because [laughs].

Yost: Did IBM provide any service personnel to help with the implementation of RACF at Travelers?

Johnston: I'm sure they did in the data center, but certainly not within the line department. I went to an IBM training class for one week for RACF. That's how I learned how to do such things as tracking violations and determining who they were, etcetera. It was a good course and I was all upbeat about RACF at the time. It's just when I saw the competing products coming along and them having features that RACF didn't offer.

Yost: One thing that came across strongly, not only with Barry Schrager, who developed with two others what I understand is the first major competing product, ACF2. But also, Worley agreed with this that RACF, was lacking protection by default, and that this was a major shortcoming. Do you hold that opinion as well, or were there other things that you saw as the major deficiencies in the first iteration of RACF?

Johnston: The primary deficiency was the amount of effort that had to be put in in order to protect specific components. And again, that's directly as a result of no default. That's where the guys in the data center that had the responsibility for that were going crazy, putting in all kinds of hours but like I said earlier, they did a fabulous job. We identified the areas that needed to be protected, we just didn't do the implementation effort, with specifically trained people, and as you suggested, more than likely they had IBM employees there, as well, guiding them and assisting them when they needed it. We just had to identify what data structures, databases, needed to be protected and to what level.

The only area that created a bit of a problem in the beginning is nobody considered one key aspect, and that is backup recovery because the security controls were perpetuated onto those tapes and now all of a sudden, you really need unlimited access when you're trying to recover that. And nobody had thought about that until we had the first data center database recovery, and it was like, what? I don't normally have access to this data and now I've got to recover it all.

Yost: Moving back to the Computer Security Institute of 1974, so the first year of that; at that first conference you said the workshops were a mess but there were some good papers were given. Do you recall any papers specifically?

Johnston: No I do not. I can certainly probably dig them out because I'm sure I've got them all but where, I'm not sure.

Yost: Obviously, you came into this organization from the insurance industry. What other industries were represented and can you give me some idea of the relative mix them, of banking, finance, or manufacturing ?

Johnston: Banking was definitely there. Nothing having to do with the financial services side, which is Wall Street, that I recall. The other big presence was the major manufacturers, and I'm talking about Pratt Whitney at that time, because there wasn't a United Technologies back then; Grumman, Boeing, [pause]

Yost: Were the auto companies represented there?

Johnston: Auto companies didn't seem to have much of a presence for a couple more years. We understand why the military manufacturers all got in on the boat because they got read the riot act from the military so that's why they were trying to learn all they could and rapidly became good contributors. The auto companies, I suspect, just didn't have much interest until they found out that this was a way for their competition to possibly peruse what they were doing in development work. That's just speculation on my part.

Yost: Did any military personnel participate and try and influence or shape directions so the contractors would be adhering to the type of policies they wanted?

Johnston: None that I noticed. It's possible that some were there in civvies; sometimes while I was working on a project and specifically the one in 1991 through 1995 in New Hampshire, I couldn't go to a conference, based on the name of the company I was doing work for. So I had to form my own company. The military did that, also. They had somebody just pick up a business name and that's how they would register at a conference because the supposition at that time was that the military was coming here to learn who the hell's teaching them, what's the condition of things. And I experienced that in the reserves. Fine, you're going to a conference; don't mention you're in the military. There's good reason for that, as well. The simplicity of it is here I was, by the mid-1970s — I'm going to say the later part of the 1970s — one of the leaders in implementing

computer security and I kept telling the commander, I need to go down to Washington and help them out; or I need to down to first army and help them out. I always got turned down, which was a disappointment to me because I think I could've made a difference. The Army was very slow in computer security, and I simply didn't have any influence until I became a warrant officer and then the story really changed. All of a sudden, I was responsible for computer security for the division, which was all of New England; I had to go into various places, make sure that they're following procedures.

Yost: Do you remember when that was?

Johnston: That would've been 1980. In the military, you can't get an appointment unless there's such a position vacant. And when the division, which was more or less a ragtag training division without any mission, suddenly got assigned as first level mobilization. Most people said why would a training division be top level mobilization? The answer was we were assigned to Fort Campbell, Kentucky, and their division had become top level mobilization, somebody else had to take over that base. Can't leave that base unattended, number one; and number two, gee, you can conduct training from there. So all of a sudden, we had to be there before they left, so we actually were in a higher priority than the Fort Campbell staff. That was really interesting because all of a sudden we're going to have to jump out of bed and get going. And the real interesting part of the whole thing was the first year we got the assignment, we didn't go down there to train; only the key staff, in order to learn the facility and that sort of thing so that you could plan the transition for the following year. My AG, or most people prefer G1, who

obviously reports directly to the general, insisted that I go, which I didn't mind; I was looking forward to it. The commanding general says no, I don't need any lowly warrant officer tagging around with us. The AG just kept on his case, said Mr. Johnston you're going if I have to take you in my car. [Laughs.] Anyways, the commanding general relented and when we started heading out to the first building, I heard him tell the sergeant major to make sure the warrant officer is back at the rear of this. We went into the first building, computers, they started talking about the computers, the general played like he knew what was going on, didn't embarrass himself at all. We came out of that building he said, Mr. Johnston, I want you right behind the sergeant major so you can help me out. So he suddenly got a real appreciation for how much computers were going to play in the mobilization. All of a sudden, now, that sort of increased my prestige back at home base, as well. I used to get questions, and sometimes when I wasn't on duty I'd get a call; he wants to know this; fine, I'll get it to him, of course. That's still in the early days of everything; there's no internet for electronic communication or anything.

Yost: You're still in industry so you're just putting in reserve work on weekends?

Johnston: That is correct; or nights. I mean, the standard training organization is one Sunday a month and four week nights a month. So you get five days' pay for a month's worth of work. We didn't mind it; it was a nice little supplement; and we had set the objective that I was to get a military retirement. I'm going to tell you, with everything that's going on with health care and everything else these days, I'm sure glad we made that decision. We still, other than a little co-pay for prescriptions, don't pay a penny on

medical care because what Medicare doesn't pay, TRICARE does. Anyway, that's getting off the track a little bit.

Yost: When you went to the Computer Security Institute, at that first meeting, roughly what size was it? You said there were about a dozen workshops?

Johnston: There were twelve workshops, exactly. And the attendance was in the low 200s.

Yost: Can you give me a sense for how it grew, say, in following half decade, up 'til about 1980?

Johnston: By the 1980s it was well over 1,000; maybe 1500.

Yost: Through that time, was it *the* place for answers?

Johnston: It was the only place. The only other conferences, were by ACF2 and Top Secret, who started running their own conferences. I used to follow the Top Secret conference in the 1980s because that's what I implemented at Phoenix Mutual and I went to their conferences.

Yost: Was there a RACF conference?

Johnston: If there was, I don't remember it.

Yost: Or might have that been part of SHARE?

Johnston: I believe that was part of SHARE and keep in mind, IBM still, in those days, was running a good number of training programs — they actually called them schools, for heaven's sake — on their own campus. I think they felt they had better control, too, that way. They knew who their instructors were; they were their own staff, exclusively.

Yost: Did you go to any of those IBM schools?

Johnston: The one I mentioned on implementing RACF. No others come to mind.

Yost: So was it in the first year, second year, that you started running the workshops for CSI?

Johnston: Second year, yes. And I implemented it with 24. Then John saw how it was; workshops that were drawing a crowd; and it got to the point where he couldn't let anybody who wanted to go, go, because there just wasn't the space. And some of the instructors would limit the number as well. So then he asked me to do 36; then he asked me to do 48. I did 48 for two years and I said, John, this is too much. You've got to understand the amount of effort that's involved. I'll be glad to work one year side by side with your staff member. I was really telling him you need your own staff member to do

this, I said. You can still have a workshop chairman or whoever you want to name who can review the courses once they're submitted for consideration and that will help but you've got to have a dedicated staff member. This is undoubtedly what's generating your revenue anyway, so there's no reason why you shouldn't have a paid staff member. And that's what he did. It was only a few years later, sometime in the 1980s, he then sold it and it's now based in California.

Yost: So you had a call for proposals, for the user workshops. Did you also aggressively recruit from people who you knew would be good to get to conduct a workshop?

Johnston: Very much so. We put a call for workshop papers in the various periodicals, and it's very much like it's done today; send me an outline; what are you going to cover? How many pages? That sort of thing. Don't send me your story, yet, until we see whether it fits into the program. The basic institute program usually was dedicated to a particular facet of computer security, primarily, like contingency planning. So if we've got 24 workshops, probably you want at least six, possibly 12 of them, to address various aspects of contingency planning. It's always interesting, when you start talking about contingency planning, and then you talk about business resumption planning. They say well, isn't that contingency planning? No, this is one aspect. Too many people have a disaster recovery plan but they don't have a business resumption plan. That's addressing the business side of the community. What happens when you lose all the equipment in an office building? How do you get it reset up, etcetera, etcetera? Oh, I see your point. We may have to have emergency access, etcetera; all of that's got to be taken into

consideration. When I first started insisting on business resumption planning at Phoenix Mutual, there was massive resistance. Then when I got appointed to director and at senior staff meetings all of a sudden everybody says, hey, when are we going to; when are you going to come address it for us? [Laughs.] So. But in the beginning it was just something else getting in the way; they didn't see the benefit of it. You'll see the benefit, if it happens. We used to test those, which is interesting; move a department into the cafeteria, because the department's been damaged. Now all of a sudden, you've got operations realizing hey, they got to put the connections in so that they can move the equipment there and hook it up. Oh, son of a gun, there's more to this than you realize; we can't just move the department to the cafeteria. I still know many companies do not do a business resumption plan and to me, it's a disaster waiting to happen. In today's world, you could have so many of those people do that work from home. You know, there's all different kinds of ways. The resolutions today for that are just phenomenal, as opposed to what it was in the 1980s.

Yost: What were some other pioneering areas of workshops in the 1970s with the Computer Security Institute?

Johnston: We started offering security courses on the various security products, not designed to compete with their own, but rather to have a appeal to those coming in that wanted a breadth of information; to still get some focal points on the product that they have; and they want to hear that from someone who has already done it. They don't want to hear it from the vendor, they want to hear it from people that have implemented

because their perspective is totally different from the vendor's perspective. That helped a lot. We started seeing; not computer security managers, they were already there because of all the responsibilities; we were starting to see the technicians implementing the particular product, suddenly getting an understanding of the entire world of computer security rather than administering RACF, or ACF2, or Top Secret and saying gee, this is an interesting world. It's much broader than I realized. [Laughs.] More than one would come to me and talk to me about what was going on and what did they have to learn in order to; so I started doing a course on how to become a computer security officer, which was very popular. There's just so many different aspects to this. I thought about — we never did — about, you know, managing computer security, because this gets more into personal attributes. How do you talk to top management; how do you present positions; and that sort of thing. That takes a couple of whole semester college courses to teach that, not just a two-hour or one-hour workshop. There was one course, "How to Be a Computer Security Manager," that I actually suggested that they take specific courses at the local college in order to improve their personal skills. It had nothing to do with computer security, it has to do with your personal skills, and I got criticized for that by some of the attendees. I said well, you don't have to take it if you've got the skills already. This is targeted for the people who are here that don't have the skills and are smart enough to realize it.

Yost: Were there any elements that you saw as industry specific to insurance and were workshops ever designed that way, or were they broader, crosscutting themes that would apply to many different industries?

Johnston: In the beginning, perhaps, because who had nationwide networks? Initially, it's was only the insurance companies; initially, it was only the Travelers, for heaven's sakes. As the banks started doing remote management; but you see, that's actually moving into the 1980s, not the 1970s. When the banks started doing remote management of their branches you started to see some of that. In fact, in the late 1980s; oh, never mind. [Laughs.]

Yost: One of the things Willis Ware followed his Defense Science Report with was working on several committees dealing with privacy. The group that provided recommendations that resulted for the Privacy Act of 1974, and out of that act came the Privacy Protection Study Commission. We have Ware's papers and I know that he brought in people from the banking and the insurance industry. Did federal legislation with regard to privacy, even though much of it was directed at government, did that have any influence whatsoever, in terms of thinking about the records of clients and the protection of private information?

Johnston: Not very much. First of all, generally speaking, they felt that the security they had preserved the data and to limit access to the data was sufficient, and without any specific guidelines, why were they going to wear themselves out? The one area that got most impacted was human resources, because prior to that there was very little in the way of protection. So they got impacted the most. Generally speaking, access to the personnel information was available in all the departments. Only for specific people but there

wasn't any guidance regarding printing it out, regarding making copies of it, that sort of thing. If we were to talk about it today it would be a totally different story.

[BREAK]

Yost: Travelers purchased RACF early on. Was the pricing of the relative early computer security products a factor at all in making a choice?

Johnston: They didn't exist. They didn't come out 'til later. It's right around — I'm going to say — ACF2, if I remember correctly, was introduced in 1978 but didn't have any meaningful hits until late 1979, at which time Top Secret came out and Top Secret was easier, in my opinion, to implement than ACF2 so it rapidly grabbed some market share. When the Travelers got RACF, there wasn't any other choice. To my knowledge, they're still using RACF today. It's probably because it would be too much of a monster to try and rip it out and use something else. Like I say, they have a master contract, I mean, it was IBM's database that they implemented. And like I said, they were the first national database in the country. Didn't know I was going to work for a pioneer when I went to work there, but they were.

Yost: Do you know roughly when the other insurance companies started implementing nationwide databases?

Johnston: Let me think about this for a second. By 1980, probably stepping back a few years; probably about 1978, the Hartford did. They had built a new data center, and a backup data center three towns away. Crazy, but that's what they did. If I had been there, it wouldn't have happened, but; one good blizzard [laughs]. Anyways, so about 1978 for the Hartford. Phoenix Mutual had a very limited network across the country. I say limited to the extent that it was essentially one terminal in each office, and it was mostly the query type. You know, somebody's making a claim, let's find out information on their policy. That was about all they did at that time, and that was done also in the 1970s. As much as anything I suspect, by that point, they were all doing something to make their agencies happy that they were going modern and there wasn't a real lot of effort at it. Phoenix, in particular, decided at one point in its history to go heavily into commercial insurance lines. After all, they were originally nothing but a large insurance company, Phoenix Mutual Life. When they went into commercial line sector, that demanded national access to everything. I had already been; I was the security manager at the time, I hadn't become director yet; I was heavily involved in that implementation, as far as what controls had to do, what-have-you. They, on the other hand, brought up the backup. The data center is located in their building and I don't know whether you're familiar with their building or not, it was the original two-sided building in the world, very interesting building to be in, especially if you sit in the point. Anyways, the data center was, and still is in that building. When we went to commercial lines, I said, we gotta have a backup data center; you've got to remember the feet of this building are in a floodplain. Yes, we're protected by a dike, but when's that going to happen? We put one up in Greenfield, Massachusetts, a wee bit further away [laughs], and that was kind of fortuitous, it's

almost like I was a soothsayer. Now only were we in a floodplain, we were down a very steep hill. One of those torrential downpours flooded the parking garages and started approaching the center. [Laughs.] Needless to say, the only thing that got knocked out was a couple of transformers in the parking garage. But we had the backup data center and what little needed to be processed was processed from there. That was a real live test.

Yost: There is one other area that I think there was a nationwide networked database system by that point, and that's airline reservations, Sabre and its descendants, which IBM worked on. Did that have any influence, any learning from that project on the part of IBM that influenced its customers in other areas such as insurance?

Johnston: Not that I know of.

Yost: In 1981, the *Computer Security Journal* was launched. That's a journal of the Computer Security Institute.

Johnston: That's correct.

Yost: Can you tell me what you know about the history of the formation of that journal and I see that its original editorial board included people from industry — insurance, banking — the original editor-in-chief was an attorney; and it also had some academics such as Dorothy Denning.

Johnston: It was a wonderful endeavor. I was a contributor to that first journal, and twice afterwards. The editorial board was, I will say, very careful in their reviewing of the proposed papers to ensure that they were accurate. I can recall being contacted once or twice about something that I had put in my particular submissions. One time I was asked to reword it, I said okay; we're convinced you're right, now let's try and word this a little bit differently so that it's more palatable. And in another case, once I explained it to them and gave them another reference, nothing more was said about it. I do know that they were definitely carefully reading these papers before they were going to be published. That's what made the journal such a success was its accuracy and reliability.

Yost: Do you know, did they use outside reviewers or was it the editorial board that took the lead in evaluating and insuring accuracy?

Johnston: First cut was always done at CSI. By this time, they had gotten to the size of staff where they had one floor of a building, as I described, and I think that was more for format. You didn't; there wasn't any specified format to submit it in, they would; those who weren't aware of what the expectation was would get it back redone because they would have to approve the new format before it went on to technical reviewers. There was one technical reviewer on staff but often, he didn't know the subject matter that was being presented and those would then, in turn, be sent to various members of the editorial committee for review. John O'Meara was a very thorough person and he wanted to only put out the best; and I think he very much succeeded at that.

Yost: Do you know if most of the articles just came in, over the transom submissions or unsolicited so to speak, or was a lot of material recruited?

Johnston: A lot of it was recruited, keeping in mind that at this time, you've got 48 workshops as a source, plus all those presenters at the prior conference. You could directly solicit based on the reviews of the workshop or the presentations.

Yost: There weren't proceedings published from those, so the best of the content wound up in the journal.

Johnston: Exactly.

Yost: And how did you; to what extent did you see changes with the journal in its first decade throughout the 1980s? Can you talk a bit about how it evolved in that first decade?

Johnston: Well, initially, first of all — I think it's year one and two — there was only one publication. Starting year three, there was a spring and fall publication. As much as anything, that's [because of] the availability of good articles to publish. The first one was somewhat thin; the second one was hefty; and then you get two hefties after that, each year, which suggested that a lot of work was being put into them. I did find that once they got to twice a year, then often there was only one or two articles in the publication that I really wanted to spend the time to read. I usually would skim all of them, simply to see if

there's a hint of something in there that I ought to know. But if they're off talking about a particular product that I don't have any involvement with then I'm not going to spend the time to read it. So, like I say, I never saw any falloff in quality. A few times I've noticed an article that I thought didn't answer a question that should've been answered and I would, rather than embarrassing anyone, I would contact the author directly and ask is there any particular reason you didn't address this particular issue? It's a way of keeping friends and they can decide whether they want to do it. What I started noticing, not only because of what I wrote, because possibly what other people wrote authors; that the next issue would have an addendum to the previous article, which I thought was very credible on the part of the author and on CSI making sure that that additional information was made available.

Yost: The same year that the *Computer Security Journal* starts, the IEEE started its Security and Privacy Symposium and published proceedings from that. For the most part, that wasn't very industry focused.

Johnston: Right.

Yost: But did that have; was that an event you ever attended? Did it have any influence that you saw on industry development?

Johnston: IEEE Conference tended to appeal mostly to the audit community, not so much to the information technology people. It also appealed to a number of senior

managers who had taken an interest in the IEEE because of some of the other courses that they offer. I attended one and was disappointed, so I just didn't go again; that's what it amounts to. I tend to read; I get their publications and who knows? Maybe they'll come up with something I really want to know. Right now, it's kind of hard to get me off course from my primary interest, but who knows?

Yost: You mentioned that Travelers is probably still using RACF and indicated that there was; or at least implied, as I understood it, that there were significant switching costs once you had a system in place. Can you talk a bit more about that and did you know of instances with other companies that ever switched from RACF to ACF2 or Top Secret? Or was there just a really strong lock, once a system was in place?

Johnston: I spent a brief period of time — a little over a year — was it that long? Probably not; with Hartford National Bank/Shawmut Corporation. It was just prior to my taking my position in New Hampshire and that was during a period when Hartford National merged with Shawmut Banks, making it a very large regional bank, one of the largest regional banks around. Hartford National Bank used RACF and Shawmut National used Top Secret. It was kind of interesting because here I am at Hartford National, Shawmut's implementation of Top Secret was guided by me as a consultant. So it was a real simple transformation for me. I knew enough about RACF in order to do the transition for them over to RACF. I was sort of sitting pretty, you might say. The worst part of that job possibly was when I finally had to tell the security people, guess what, you're moving to Hartford or you don't have a job. I knew all those people by first name

but that was a part of the situation. I was a — somebody might find this interesting — you're sort of sitting pretty, why would you even consider another job? Living in a good community, own a home, all that good stuff; have to move all that stuff. An investigation was conducted by yours truly, for the audit department, of three executives of financial misdeeds. When I got done, I wasn't told a thing about what was going to be done. I inquired, nobody would tell me, but one of those people was the chief information officer and I was one level removed from him. And I'm saying I don't know what's going to happen here. In fact, he did some queries to me, almost as if to say, what do you know about this? Of course, you skirt the issue; dance around it. And that just got me worried. I got called by a recruiter for this position in New Hampshire; they were going to pay me a lot more; yaddayaddayadda. So I looked at my wife and said, guess what? We're moving. She says, oh why? So you have to go through that whole thing, but at least the kids were out of the house at that point. So we made the big jump. One of the major national banks bought them out; I probably wouldn't have been able to stay on after that, anyway, so.

Yost: Thinking back to the decade that you had with Travelers, was it difficult at times to get policies implemented and the resources you needed from central management of the corporation? And how did the voice of you and other top security managers for Travelers have with management, how did that change over that decade?

Johnston: [Editing Note: You asked about the Travelers but I answered for Phoenix Mutual…a decade later!] Well, it went through several transitions. First, I was reporting directly to the chief information officer. After about a year [pause]

Yost: There was someone with that title way back in?

Johnston: Oh yes. And after about a year, he had me reporting to his vice president, which didn't impact me at all. But I was having the problems that I talked about earlier, of getting policies through. So in about 1983, there was a separate division of IT called the PC division. We were just getting into installing PCs and I was being transferred to that division; reporting to the head of that division. I asked the vice president why I was being placed there and he said, it's simple, you've got the security skills. This is a new era and we need somebody who can manage that, make sure that starts from day one rather than an add-on. Fine. It was at that time that I bought a PC junior, [laughs] which was about all I could afford. I think I kept that thing for about a year. That's what led to my publishing career because now I had a computer in my home so I could write. But most of my influence for the next year or so had totally to do with PCs, managing PCs from a security aspect. It was fun, it was challenging because at first, while I'm learning new things, I'm looking at new equipment, considering security software, etcetera; as well as procedural because we were worried about the PCs out in the departments just as much as we were within IT. There wasn't a lot of resistance to securing the PCs, and procedures went through rather readily because everybody was — for lack of a better term — afraid of these new monsters. So that went rather smoothly. It's when I got appointed as the director and we got into the backup and recovery, and the fact that we needed to have a backup data center, and all those procedures, for quite a while met a lot of resistance in the line departments. And that gets back to the point where I could; get on

the docket of every executive committee meeting to make a statement. The position; all of a sudden, things became a lot simpler. But that lesson that I had learned — actually, I guess I had already known it — always sell the benefit and not the control. Once they see the benefit then they say how do we do it? Rather than saying well, gee, we've gotta do this and they say well; you're in a defensive mode. If you can get them to ask how do we do it, you're usually in a pretty good situation to get it approved. So that technique came along; where I learned it exactly; I guess I was reminded of it when I was mentioning the instance at The Hartford when I was doing their first policy and a good friend of mine essentially told me the same thing again.

Yost: You mentioned that your acquisition of an IBM PC Junior got you into the publishing area. In 1983, I believe, is when you started a column in *Info Systems*, "For the Sake of Security."

Johnston: That's correct.

Yost: Can you talk about how that came about and also any relevant context? Had *Info Systems* published much of anything in computer security prior to that?

Johnston: That was my big frustration throughout the 1970s and up until that point, is that there weren't any meaningful periodical computer security columns addressing the current day issues as opposed to the one little event here or there. Once I got familiar with the PC — I'd had one in the office for a year or so — but I had to get familiar with mine;

I went to *Info Systems* and suggested that I do a monthly column. They saw it as an opportunity to draw various advertising, and that proved very profitable for them. Very quickly, there were various advertisements that appealed to people worried about security, on the facing page, on the back page, etcetera. They often, once that started happening, they started splitting like; although I was contracted to do a one-page article, they would do it as two half pages so that they could get more advertising close to my articles. And I found it quite easy because there was so much going on, that I had experience to write this from. There was very little rewrite that was ever done on my articles. Probably the most interesting aspect of this was of course, they wanted me to send them a floppy disk. After, I'm guessing about six months I said, gee, you know I could submit this electronically; why do I have to mail it? And I demonstrated it to them. I had access to their system and I could just [pause]; electronically transfer. They said well, I'll tell you what, you can do it electronically, but send us a floppy as well, as backup. I said that's probably a good idea. Let's keep one thing in mind, when I complete the transfer, I said, and I will call you to tell you it's there, you can do a backup immediately as long as you can read it. If there's something wrong with it, I can re-transmit it. I said, that'll be a more efficient way, but for six months, I'll send you a floppy. After three months, they called and said don't bother with the floppy anymore, nobody knows what to do with them. They're making the backup, of course, on their online system. We were doing electronic transfer; needless to say, it wasn't e-mail, but direct connect. And that was, of course I was the first one who ever suggested that. No one had ever done it before so they were a little antsy about the whole thing and so we

made it work; and I understand that they got virtually all their columnists to do it that way after that because it's just vastly more efficient.

Yost: In scanning the pages of *Datamation*, it seemed there were occasional articles on security but nothing of much substance. Am I correct in this?

Johnston: Right.

Yost: Did your column in *Info Systems* open up the pathway to other articles in that publication . . .

Johnston: Yes.

Yost: . . . or was it primarily a stand alone for a long time ?

Johnston: Even much to my surprise, so to say, I would write a particular column about a particular subject, such as contingency planning or something like that; and sometimes they would ask me, can you write another column? We need a month to prepare for the contingency planning column because they either got another columnist to write a more detailed article on an aspect maybe they'd asked them previously, I don't know. One or two cases I recall it was actually one of their staff members who wrote a particular examination of some particular issue from; and so there was some flexibility there but generally, I had two or three columns written when I submitted one so it wasn't any

problem for me to just pop another one out. There are only two or three columns that actually took two or three issues to complete. I wrote them as such in the beginning and that was the only time, of course, when you couldn't interrupt it.

Yost: And contingency planning was one of those?

Johnston: Yes.

Yost: And the others? Do you recall?

Johnston: Not off the top of my head, no.

Yost: I'd like to bring up a few of the topics that you wrote about in the first year or two. One was threshold alarms. Could you talk about the significance of those?

Johnston: I had devised that concept shortly after I got to Phoenix, and I wanted management to be aware of what was happening, in terms of time. So I started gathering specific facts and how many times; how many violations against the XYZ database, how many data compromises; and first I presented them as numbers and I quickly got told numbers are meaningless. You've gotta do it in terms of percentage so we can understand it; and shows us the percentage of increase or decrease so there's some guidance for management. So I did and when I did my monthly report, there was this little section which I called threshold alarms. Gee, security violations in the XYZ department have

been rising; perhaps some training or something else is necessary, that sort of thing. So that was the concept; that's what I was presenting in that particular article, is that gee, you've got to go to where you can collect information that show trends, positive or negative, in security. I think one of the things I mentioned in the article was how many compromises to the data center perimeter were there? Suggested, or, you know, management would get real antsy about that one, even if it was only one! And it's just as well to put that in there and just have zero; zero percent. So the concept, again, is simply, where is there data that you can reliably collect each month and present in terms of information as to trends, whether they're positive or negative. And I've used that ever since. I'm using it today. One of the things that it does for a security manager is that if there's a growing trend, negative trend, it gives a security manager much better position to say, whether it's training or a procedure that would help reduce or thwart it. Also, what it's very useful for is the manager of that department because now you can get a top manager to come down and say hey, this shouldn't be going on, your people aren't playing the game by the rules, meaning that the rules are already in place. Rather than springing it on management all at once, hey, we got to do something over here; if you've got the trends and you could see them going up over the months and finally you take the step, they're more than likely to say yes, we should've done this sooner. You don't get the resistance. That's what I like about threshold.

Yost: In another article in *Info Systems* in 1983, you had a pie chart and you showed that EDP knowledge was really as important as security knowledge. Can you talk about the

significance of that, and was that a serious problem that people did not have the necessary EDP knowledge in the field?

Johnston: The answer is, in those days, it was mandatory. You had to have the EDP knowledge because you had to do some of the work yourself. Skill sets amongst all the people around simply weren't there so you had to be able to do it or teach somebody else to do it, it was that simple. Is that necessary today? Not necessarily. Some shops it would be, others not necessarily. I saw, in the 1980s, a business manager be put in charge of computer security and be an utter failure because what they asked for, what they wanted to do, wasn't practical. The objectives were good; the method wasn't there. You can't say we're going to secure this, and this, and this, if you don't know the underpinnings, the architecture, it doesn't work. Generally speaking, in the 1980s, if a business-type manager got the job of computer security, management quickly decided this was a poor choice for that job because it just doesn't work out, in those days. Today, it can. An educated man with good common sense, in many companies, now is managing computer security.

Yost: You talked a bit about the big three security products, and wrote a lengthy article in the pioneer issue of *Computer Security Journal*. I wonder if I could mention a couple of the others and get any comments you have on them. "Secure IMS"?

Johnston: Secure IMS was an interesting tool, and clearly it was for securing databases, it didn't cover the entire environment. And that was to answer the paranoia of companies

implementing a database across the country. It did the job credibly, but unless the company wasn't going to put in another security product to do the general service, it tended to get in the way if you had a secondary product that was doing the overall security. A few companies kept it for several years but it's not around anymore.

Yost: What about Protect CICS?

Johnston: Now you're getting into my second article, really, because that was dedicated strictly to CICS protection. RACF did not address CICS and a lot of the other products didn't do a credible job for CICS. CICS is its own beast and still is today, so you could put a dedicated product on it. I haven't heard of Protect CICS for 20 years. Its concept was good; it did a decent job; but a small company; I suspect it probably got bought up by one of the bigger companies but I'm not aware of whom.

Yost: And Boole & Babbage's Secure?

Johnston: I liked that product; I truly did. The name of the firm sort of gives you an idea of the technical competency of it.

Yost: I interviewed Ken Kolence a while back, who was one of the two founders.

Johnston: Trying to think. I know I implemented it at Phoenix and it did a nice job. I enjoyed working with it.

Yost: In 1983 you wrote, "As computer security more directly affects society, security controls will be demanded by the public." Did you see that play out or were you disappointed that the public did not become concerned enough with security?

Johnston: I was concerned about it. I was hoping to possibly stimulate some of it. But the fact remains that until the 1990s and the internet came about, there simply was very little, if any, concern by the general public about computer security. That's the big corporation's job to deal with, and I trust them. Keep in mind that that was an era when generally, people, everyday citizens, trusted the corporations. After all, if they didn't do a good job, they weren't going to survive so I'm safe. It was the mid-1990s when the internet as we know it today came about; that people started realizing the exposures and started getting concerned, as you well know. Until recently, it didn't really rise to enough until the malware started attacking them, and then all of a sudden, people started really getting worried about the protection of their data. And, of course, NSA has helped that a lot, too. [Laughs.]

Yost: Fairly early on, James Anderson, Jim Anderson, identified intrusion detection as a research area and influenced people at SRI, where the IDES Intrusion Detection Expert System was developed. Did either IDES or any other intrusion detection expert systems from the research community have much of an impact on industry?

Johnston: Not that I know of. I suspect that within the defense industry, that it got some play, again, for several good reasons. But financial services, to my knowledge, never played much with security at all until somebody stepped on their toes.

Yost: Also in the 1980s, the DoD and NSA come together and formed the National Computer Security Center, and basically extending and furthering some initial work from MITRE, MIT, the Air Force and other part s of the research community came up with criteria standards and certification infrastructure, TCSEC, or the Orange Book. Obviously, the goal was that industry would embrace this. It was seen as particularly important to ensure standards for systems for the federal government and contractors, but did the Orange book, when it came out, was it talked about much and did it have any influence in insurance, and banking, and finance, and other industries?

Johnston: The biggest influence, in my experience, was in the banking, the finance industry. You've have the top managers, you know, I'm talking about outside of IT, going to a conference and hearing about this wonderful Orange Book. And they'd say we want to do something with it. And in turn, almost every one — I'll rephrase that — everyone that I had direct contact with who started an Orange Book program, abandoned it within about 12 months when they realized that while these processes and particular computers were accredited, they don't fit the business need. This is done by a very parochial view, and of course, that's the big enemy of computer security anyways, is you gotta fit the business needs because after all, the most secure computer is locked in a room and turned off.

Yost: In the early 1980s, Steve Walker launched a computer security business that grew quite rapidly. It was really the first large computer security consulting company, with over 300 consultants—Trusted Information Systems or TIS. My sense is that it was primarily contracting with defense suppliers and the intelligence community. Were you aware of TIS Consultants working in insurance and banking?

Johnston: No, not at all.

Yost: Within the Computer Security Institute, was there any early discussion about needs to have certified computer security professionals? I know later on, CISSP becomes a major credential but I'm interested in whether within industry there was much discussion before that.

Johnston: There was a lot of discussion, particularly at the conferences, primarily introduced by business managers saying can't there be a certification for this like there is for auditors so that I know that when I'm hiring somebody he's got the basic skills and credentials? That's what stimulated — it wasn't ISC^2 at that time, I can't think of the name of it but I'll use their identity — ISC^2 started in 1989 to formulate its certification program. That gives you an idea how much thought was put into that and the money that was spent just to get it started because they didn't start awarding until 1994, possibly late 1993. Essentially, you got access to their database, which I do have; nobody got it before 1995. The only reason for that is because that's when the database was built, okay? I got

mine in September of 1994. I was a part; you couldn't validate other people — prior to the test, now — you couldn't validate other people until you got your certification. How they made the decision on the first dozen, I don't know. But all of those grandfathered people, because they weren't tested, were expected to investigate candidates for grandfathering and make recommendations, and then once the test came out, the only other thing the grandfathered person was expected to do was to validate the test. We all sat down and took the test to validate it and get the perspective. You weren't endangering your credential in any way that you had earned through your experience, you were validating the test. So they went through a lot of effort. Today, it's 50 questions of the 250 questions that are on the exam, are only validation questions; they want to see what percentage of people are completing this successfully, as it were. And so questions don't even get out as a part of your examination when you're a candidate, until they've been validated.

Yost: Were there any other trade organizations that were heavily influential to you or others in the insurance and financial industries with regard to computer security in the 1970s and 1980s.

Johnston: One other thing that did come about, ISSA came along. I could look it up, but it started as a trade group in California and I don't recall the name of it; and then they decided to go national. They'd been very successful; they do a decent job; their biggest problem as far as I'm concerned is they're not involved enough in their local chapters and a lot of the chapters — I shouldn't say a lot because I don't know "a lot" — I know that

some of the chapters flounder. It's true in some areas because it's the nature of the population there. I won't say anything more about that. Other chapters have been extremely successful, which is still called ISSA New England because when it was formed it was the only ISSA chapter and it was servicing all of New England. It's still called ISSA New England, but it's the Boston chapter now; all of us know that because there are chapters all around New England. Very successfully done; and the key to that particular chapter was the intensity of the management. There were regular management meetings and you were a volunteer, but you had certain duties you were expected to perform and you would be called to task if you didn't get them done; even replaced, in some instances. To be on the board of directors of ISSA New England is a prestigious position, as a result, because everybody knows that. I served on it for several years. When I went to New Hampshire, they were convenient enough for me, because I was in southern New Hampshire, to go to their meetings and so I quickly got heavily involved and worked with them. So I think a lot of ISSA, and I do know from firsthand experience the fact that they don't get involved enough in chapter management because some chapters just flounder continuously.

Yost: And did the Computer Security Institute quickly develop a chapter structure or was it strictly a national [pause]

Johnston: No. Computer Security Institute, its membership is national and all it has is the conferences and the journal. Becoming a member gives you access to certain documents that you won't get to, even if you go to a conference or subscribe to the journal, so there

are benefits to belonging. They're off of the beaten track for me now though, because of where my focus is.

Yost: I'd like to ask a question about the encryption area, in that coming into industry, did the company, RSA Data Security and competitors down the road have a significant impact on the insurance and financial industries?

Johnston: Oh, absolutely. Particularly because when we got; it really had its impact the moment the internet as we know it came about and they wanted to have secure communication over this broadband network, particularly for their financial transaction, which obviously, is banking and financial services, but also for the insurance companies, people making claims — because now you can even put your claims in online, for heaven's sakes, but that wasn't [the case] back at the beginning of the era, in the 1990s — but their own communications they wanted to secure. Although, as you're probably well aware, https did not come into its own very well until the mid-2000s. Even my wife knows to look for that when she's doing anything, and she looks to make sure.

Yost: That company also, with its leader James Bidzos, launched a conference that was rather small at first, but has grown into a massive trade industry event. Did you attend the RSA Davis Security Conference?

Johnston: No, I'm not a fan of going to California, that's the short and simple of it.

Yost: Long flight.

Johnston: It's a long flight, and I was offered a job in California at one time, and once my wife and I did the analysis of it, we decided it wasn't worth it. We didn't like the lifestyle or anything else.

Yost: Do I remember on the resume you sent that you worked for a Palo Alto company in the early 1990s?

Johnston: Two companies, actually. I worked for Hewlett Packard, and . . .

Yost: In 1999-2000 for HP, and 1991-95 is Arbitration [pause]

Johnston: . . . Arbitration Services Corporation and Hewlett Packard. Hewlett Packard was an early pioneer in home office and they bought me a desk and everything, for my home in New Hampshire, even though the office I worked out of initially was down in Massachusetts, as you would guess. I was one of the first people to be implemented [with telecommuting]; they didn't have enough space. And then later, I was working out of an office in Virginia. Unless I was on the road, I was working out of the house. They were truly an early pioneer in home office. Arbitration Services, we had the data center in Hampton, New Hampshire and I worked there mostly for very good reasons; but I had remote access so it was; let's put it this way, most of the time I didn't have to go in at

midnight if there was a problem, I could usually deal with it. That was my first cell phone, by the way. The first thing they did was buy me a cell phone.

Yost: Off the recording, before we got started, you mentioned the IBM Fujitsu case. Can you describe that and set up the context, and then tell me about the forensic lab that you managed.

Johnston: IBM sued Fujitsu about 1985 for compromising various components of their operating systems and incorporating it in their own mainframe software. Amongst other things at that time, they were becoming a major mainframe provider and very quickly Fujitsu said we don't want this in the courts so they went to binding arbitration. Arbitration Services was formed; an attorney and an IT person were two directors; for the first three years it was a secure data center directed in Japan, run by Arbitration Services, containing only — correction — contained both Fujitsu's and IBM's software so that at that point they could identify components of the IBM system and then be licensed and paid for it. That's the key. All of a sudden, they're letting them do it, but they gotta pay; and they paid royally for it. At some point, and this is just prior to my coming into the picture, IBM decided that they were doing more than they supposedly were requesting and getting approval for. So they decided to go to the expense of building their own data center. There were a lot of strict requirements; it couldn't be near any IBM facility; so it had to be a totally free-standing facility. They found this building in New Hampshire in an industrial park — Hampton, New Hampshire to be specific — and they rapidly converted it to a very secure forensics lab. Of course it wasn't called a forensics lab at

that time, but that's in fact what they were doing because the researchers, the examiners, were going through Fujitsu code seeking IBM code. And then, of course, they had to go through the full determination; was this one of the ones that was licensed to them? It was a big, arduous process. I got hired after the facility was designed, before it was completed. I was involved in the final acceptance and the touring before it was implemented. Very interesting. I liked where it was located because it was just another industrial building. Nobody had any idea. There was all kinds of concern about radiation and the possibly of scanning. The exam rooms and the data center were all lead-protected; the walls. And there was no exterior wall. In other words, around the entire perimeter of that particular area where security guards would walk around. If I remember correctly, it was a four-foot-wide corridor, before you could actually reach anything, which, of course, eliminates a lot of other possibilities, and no windows at all in the exam side. You had the reception area, conference room, and cafeteria — bring your own food, but they called it a cafeteria — and the guards' desk. That's all windowed and I think there was one or two windows in my side of the building, now that I think of it; yes, there were, but they were in the exterior portion. I didn't have any windows either. Fujitsu was very sensitive about the fact that IBM had full access; and I mean, IBM employees had full access to their code, so controls were extreme. Anyone going into that area from the IBM team had to empty all their pockets into a locker; randomly, coming out, they were frisked head to toe. You never knew when that was going to happen. They had no phone line. All calls were made from the guard station. The guards could record their calls, if they want; in fact, they did; all their calls were recorded. You couldn't carry anything in; couldn't carry anything out. If something was to come out, I had to go in and approve it

for removal. We had encrypted facsimile, we had an encrypted voice line, beyond that it's fairly boring other than the fact that the rather important thing is the exam rooms could not be opened until myself or my deputy was present and opened the gate to the corridor where the exam rooms were. That insured or assured Fujitsu that somebody was on the premises when things were being opened up. Then the IBM manager could open one of the rooms. He had to notify me; we had alarms on those for control; I would know when a room was opened. He notifies me beforehand what room was going to be opened and what's going to be examined. During the course of the day, at least three times a day, I or my deputy would randomly walk over the visit the opened exam rooms and make sure that the closed exam rooms are locked. It was a very serious effort. Was it successful? I think so, and I say that because it suddenly ended when Fujitsu announced it was getting out of the mainframe business. We were scheduled for 10 years and we just missed a full 5 years; about four years and 11 months, if I remember that correctly. Not quite that many; about four years and eight months. I was surprised. I was proud of the fact that we did our job; what IBM wanted to achieve, they achieved. They didn't want the competition, that's what it amounts to. From there, I went into primarily consulting work, and now we're traversing into the next time period, which we're not interested in at the moment.

Yost: Were there any models to go from in setting up a central facility? Obviously, within government, there is NSA and other organizations required security, but they had far larger grounds, a far larger secure perimeter, and probably because of that, emanations

or proximity couldn't be as close. But it sounds like this was unique within industry at the time, is that correct?

Johnston: It definitely was. Clearly, the architects who drew up using this building did a lot of research because they took the effort to best protect against emanations. Location of the building was unique; there was only one building we were concerned about. Could it be used as an attempt to compromise? I just told the arbiters, look, I'm going to go make friends with the manager there and have him show me around and see what's working and what's where. Occasionally, you know, they come over and ask what's changed. Tell them as little as you can about what you're doing; but he was glad to, because everybody was going what's this group do? They'd see the guard walking around the building at night. Not in that corridor, but literally, we had them walk tours outside, too. Boy, when our equipment came in, and our inventory, keep in mind that was a headache. When the inventory came in you have to make sure that you account for every single bolt and piece. Sure caught their attention; they'd see that stuff coming in and making a record of everything that's walking into your building. There was a data destruction facility down in Massachusetts, and when we had material that had to be destroyed, either myself or my deputy would go on that truck and someone else would follow us, and stand there, in that place, while they destroyed it. There was no chance that it wasn't properly destroyed and that was an arduous process when we closed. There was a lot of material that had to be destroyed. Fujitsu didn't expect their manuals back or anything like that, they just wanted to be sure it was properly destroyed. I had a full time deputy, and then I had a backup; someone I knew who runs his own security business

today in Massachusetts. He's supporting RACF, now that I think about it, and has several contracts doing RACF work. Beyond that, I had a fair amount of leisure time during work hours. Get up and walk over, inspect, make sure everything is right, check your inventory, that sort of thing but it's not like it took eight to 10 hours a day, it was more like two or three hours a day. So I got, as I have indicated, very heavily involved in ISSA. I can't think of the name of the firm that specializes in physical security, just doesn't come to mind at the moment; it was a local chapter. I had never belonged to it. Amongst other things, I wanted to see how many of the guard companies or guard companies' management [belonged]; and I got to pick; they gave me three firms and I got to pick one. I wanted to see how many of them were actually going to some of these meetings. So you're learning a community; you're learning all different subsets of people; one interesting comment I got was from Johnson Controls. They took care of all of our security software and hardware, and I got it from three different people over a period of time; haven't seen a facility this secure and they're doing the military bases in Massachusetts.

Yost: Fairly significant defense contractor.

Johnston: Yes. It was just; and they sort of knock you over a little bit when they tell you that. But it was; it was well secured. We had motion detectors. This was a high; originally was a warehouse; had high ceilings for plenty of stock, what-have-you; so we had false ceilings below that and we had motion detectors up there to make sure somebody wasn't crawling up through the false ceilings to get over into our area. Of course that created a

problem once in a while when a bird or something came in. [Laughs.] I got a big kick when IBM came to examine the facility, and the lead man came and started throwing up ping pong balls. He said, the alarms don't go off. I said, it doesn't have any body heat; we don't want false alarms just because a breeze stirred up. I specified that it's got be both motion and body heat. He says, oh, okay. I'm not going to let a bird go in here.

Yost: Can you tell me about your background in forensics and how you developed the knowledge base to get that leadership position?

Johnston: After the position in the Hampton facility, I started doing consulting work. Most of it was to the financial industry based in Massachusetts, primarily downtown Boston. They wanted to have network penetration tests done. That got me very much; prior to that, I had little to no experience dealing with networks so I had to do a whole lot of studying of networks to understand what was going on, and then start running penetration tests. Of course, then you turn around and you tell them what's wrong and what they need to do in order to improve it. Then some of these same firms said well, gee, can you take a look at some of our applications and operating systems in order to see if they have similar faults? Well, they won't be similar, but they equate to the same thing. That was kind of nice because you're learning this stuff and being paid for it at the same time. Somewhere midterm in there, I was working for M. Corby and Associates and he had a client, travel agency, that one of the computer people was unhappy and walked off with several of their tapes, holding them as hostage. Wants his job back; he wants a promotion; etcetera. Mike turned around, said, Bob, get over there; make sure their

current network is secure, change whatever needs to be changed; see if any hacking's been done. So that was really my first forensics case, and that was done pretty much by the seat of the pants, but you learn a lot in the process. We saved — saved is the wrong word — I successfully protected the travel agency and they were forever grateful after that and stayed with M. Corby the whole time because we made some specific improvements. And I got the evidence necessary for them one, to collect on their insurance, because they had good insurance coverage and with the evidence they were able to convince the insurance company and the insurance company had to pay for the cost of my work and a few other things; and that in turn got presented to the district attorney, and the guy was prosecuted successfully. That got to be kind of exciting to me. I did another job for Corby, and that was in Washington. An agency had bought a particular software package and the competitor was then sued because that package was not as good as theirs and they were competitive in price. And so this is going up to the GSA, and they hired me to come in and do my objective compare, and see what you come up with. That took a lot of work and a lot of time in D.C. When I got done; and I also not only looked at the software, I talked to a couple of the managers as to what their expectations were; and I came to the conclusion that while Product B does have some features that aren't in Product A, Product A is the best business solution for this agency. It does what they need to do, it's easy to administer, whatever; and so there was no error, as far as I was concerned. GSA accepted that and told them to go fly a kite. Beyond that, I started reading; I started paying a lot of attention to the SANS publications; never went to a SANS course. There's something back here that tells me don't support SANS. The simplicity of it is that they started competing with ISC^2 and that's what causes that to be

in my mind. I look now much more carefully at SANS; SANS comes to Boston every year and I just may go this time because they are teaching things. I participate in several of their discussion groups and find them invaluable. So it's kind of interesting. This is sort of jumping over the fence a little bit. Getting back, ISC^2 just starting offering a digital forensics certification and once I learned how it was done, who did it, I wrote to them and said don't ever expect me to take that test, this is so baseless as to be ridiculous. The author of the course was obviously very upset with me but you have to take your stance. I just know from how it was written that; and I got a good look at it, too, they gave me the opportunity to take a good look at it because of the work I do. So.

Yost: Are you aware of the design of facilities where there was learning from the forensics lab that you led and did you do any major consulting that kind of spread expertise in that area?

Johnston: I gave a course two years ago. It's held down in Virginia; and I can't even think of the professor's name who constructs it every year. I gave a course on implementing forensics training at a university and covered all aspects of it from basic course content to the forensics lab design. It was received very well and he's wanted me back again. I felt I haven't had the time. I'm seriously considering going there this year; very possibly teach a course on the history of computer security. That certainly should be of interest to folks that are attending their conference because the majority of their attendees are professors. It's kind of interesting because with the credentials I have, everybody assumes that I must have a master's and I don't even have an undergraduate

degree. [Laughs.] I've been working on it; I'm taking courses on police work, primarily the intelligence side. Then I'm taking some secondary courses that has nothing to do with [it], Native Americans. [Laughs.] But that's my big book that I've almost got finished. My biggest conflict these days, frankly, is I'm too multi-faceted and I've got pursuits I mentioned earlier. I talked about some of the assignments I got that were outside of personnel, that I chose not to say anything more about. I've written; I've got that book about half written about those various events and I've already gotten it cleared by NSA that that's not classified anymore. Nonetheless, it would be so sketchy if I put it in this interview as to be not factual at all.

Yost: With regard to the big three computer security products that you wrote about early on, two of them were companies that were acquired by Computer Associates, and as they often did, they were acquiring to continue the products rather than the organization, the company. In your opinion, did that retard innovation or competition in the computer security products industry, that two of the three leading products were held by one company?

Johnston: In the beginning, that is to say the first two years, the answer is yes, there was not any significant improvement in any of them. They were too busy learning about the other products. They didn't even take much of the staff, either.

Yost: That was kind of typical of Computer Associates.

Johnston: Right. But as time went on, they started becoming responsive to the demands of the community, especially, coincidental to that, is the fact that RACF saw an opportunity to advance itself in the marketplace because a lot of people just didn't want to do business with Computer Associates, basically. So there were a number of converts that went to RACF. If you've got somebody who's been using Top Secret or ACF2 for a number of years and they go to RACF, they start making some real noise. You're our only alternative and we aren't all that happy with it. IBM saw the chance to really make some advances with RACF and made some significant improvements. That was a kick in the butt for Computer Associates also.

Yost: RACF gained some additional market share?

Johnston: That's correct.

Yost: Can you briefly give me a sense of what you've been doing over roughly the past decade?

Johnston: We moved back to Connecticut in 2003. At the time, I was working for ISC^2 while I was in New Hampshire, and they moved to Florida. My wife and I don't even consider trips to Florida, much less living there. My wife says well, our grandchildren are growing up and we're spending three hours each direction. Let's sell; let's move down to Connecticut. My military retirement had kicked in so there was some money to get along on. Don't need the total story of that transition. I continued my consulting work and in

2006 I started teaching computer security at Asnuntuck Community College. Very successful; very enjoyable; they liked it too. And I decided to do a course on digital forensics. I noticed that three of the people in my class were from the chancellor's office. At the time, I had no experience with Encase, so I did an overview of it, what you could extract from the user manual and I discussed all the other tools that could be used, and techniques. After about six or seven weeks, I got a call from the chancellor's office that says, we don't need you to teach that, we need you to do it. So obviously, the people that were there must have been happy with what I was teaching. They're still on staff, too, but they're not doing forensics work. And I said fine; I've got to finish this class, I'm not abandoning it. And they said that's fine. And I said, you know, I'd like to take a little break rather than just start driving down to Hartford. And they said well, how about right after Christmas, that's a nice time to drop into the bucket, so to speak. And I said that's fine, let's talk a little bit more about such a job. We negotiated things out; he didn't realize my age, I was 69 at that time when I threw that playing card in, I said gee, I don't really like driving to Hartford every day. He says, well, I can work it out; you can work from there; you'll have to come down to get the equipment. Other than that, you can work; which was fine. Obviously, we reached salary and working hour arrangements, which was flex time; and I started, you know, in late December 2009. I was supposedly only going to be there for six months; we were going to solve the problems that were hitting the university; well, at that time, it was only the community colleges. And then I wouldn't be needed, so I was on a six-month contract. I've been there ever since, always on short term contracts. It has a bit to do with labor; I'll never take a full time permanent job because unions in the state of Connecticut are so rugged, I would have to join the

union and the union will not allow any employee to work from home, it's part of their rules. So, no way. But I swear, they probably get 40 to 50 hours out of me, even though I can only bill for 30, because I do it at my convenience. A good example is over the weekend; I go to my home office two or three times, check out all the e-mails. I get a lot of e-mails I don't need; just delete them. A supporter knew that I was off today, he said he'd have a case mounted today so I could start bright and early on Tuesday morning; and what do you know? It was there this morning. But it's the one I mentioned a little bit earlier to you, so he got a nice e-mail from me. In the beginning, I was doing three to four cases a day, and it was necessary. Now, I'm averaging five to seven cases a week, and I'm doing all of them. The difference is how could you go so fast in the beginning and not go that fast now? First of all, over time, I've made them much more thorough. The model I was given I felt wasn't complete and I built a rather — I won't say exotic — I'll say a thorough model. And every time when I start a case, I push a button and basic case map is all put out into text file, and I get to fill in all the blanks. And of course, you don't forget anything because there's a cue for all the things that have to be done. Now I do something that a lot of people don't make any sense out of but it has to do with my long history with computer security. You're in there, you're doing forensics; can't you do a little bit of analysis about what has been or hasn't been done that might've prevented this whole thing from happening? So I look at certain files to reveal certain information. One of them is that our policy is that they're supposed to have Microsoft Security Manager running; it does not conflict with McAfee, they can work in tandem. I check to see if it's running or not; that's one of the things that goes into my final report, whether it was running or not. I check all the critical components. Okay, what are the critical

components? Java, Adobe products, and iTunes, and QuickTime. Those are all common vulnerability points; most commonly attacked, used as an entry venue. I find every one of those installs, when they were installed; I also look at when the image was created because our policy is that every system should be re-imaged once a year. And I get this nice summary and I can then create the management reports of the trends. Some colleges come out real good and some don't. Keep in mind this is 2012, the community colleges — I'm going to use my way, the way I think of it — the universities were merged with the community colleges under one management team. They'll tell you the other way. And he told us in the beginning, eh, we're not even going to worry about it. They quickly found out that the controls we had on the chancellor's office operating system were far superior to what they had out at the universities. [Laughs.] So, they've bit their tongue since. But we're making changes now; we have to. Things go on and get better. I do have some influence in that regard; I don't play the role; I refuse to play the role. If I see something that's really good and I can justify it and explain why this should be considered, I go to the acting CISO and deliver it to him. Sometimes I hear back from him about it; sometimes I see it being bought. So I feel I have an influence I like to have without having to get into these doggone discussion groups about it. Let him do it; he's been doing it longer there than I have so he knows the policies better than I do, as well. Politics in an organization like this, especially now that you get the four universities added to our platform, and another college, it's a state college; online college; came into our system; we've got plenty to do. All the vendors keep harassing me and sometimes I just have to tell them; I enjoy getting the information because that part of my skill set is being satisfied without my working at it. It's a fascinating; and things are changing. The

malware attacks are getting much more difficult to pin down than they were four years ago. I mean, *MUCH* more difficult. They're getting smarter about what they're doing. I hate to say that, but they are, so I have to keep getting smarter, too. I think I've had two cases this month where there wasn't any trace of how they got in. It doesn't show up in the web history; it doesn't show up in e-mail history. In both cases I finally came to the conclusion that it was an old exploit. It wasn't capable of exploiting the components I just mentioned and so therefore, there's nothing else to find. It really didn't do any damage; it couldn't. Both those cases, I took an extra step. I decided to declare it as a possible compromiser; you prefer the term, I'm sure, PCI data. It's called DCL3 because it's federally and state regulated. If you look up DCL3, you'll find all the information you want on it. I just declared it "possible DCL3 compromise." I do not do the network search. I declared a possible DCL3 compromise, he does all the research. I tell him whether or not there was any DCL3 data on that computer. I will say that unfortunately, more often than not there is, and there shouldn't be because we have a mandatory running of identity finder on every system once a month and anything found needs to be removed. I shouldn't be finding any, okay? But I did find it. That's one of those red flags I like to talk about. Both those cases supported my conclusion that they weren't successful because it never communicated out. After all, if you're going to try and compromise DCL3 data you've got to have outgoing data. But that's the part about playing it safe. If you can't explain something, go the full hundred yards, so to speak; then you can confidently say there's no compromise.

Yost: Is there an organization that focuses specifically on computer security professionals in higher education and do you participate if there is?

Johnston: I don't know of one. The only one I know of is the one that I taught at, and I'm sorry, it just doesn't come to mind. And like I said, I think I'm going to teach again this year. But I don't know, other than that conference that's being hosted by one of the universities in Virginia. And as much as anything, he creates one whale of a database online that's available to anybody once they register, and have access to; and at the end of the conference he publishes one or two symposium manuals. It depends on how much there was to publish whether there's one or two. At the moment, I think it's the only thing that has any decent size and validity, and it's definitely computer security, it's not just computer forensics.

Yost: And finally, are there any topics that I haven't asked about, or things you'd like to elaborate on before we conclude?

Johnston: Well, not really. Obviously, in the paper I'm preparing for the conference, it's going to bring out a lot of the other articles I've written. If I had found them by now, I might be saying yes. But they don't come to mind at the moment. I'll make sure that I get you copies. What I'm going to have to do for the moment — gee, I hate to admit this on tape — I had a problem with my home network last week. It had started; and we finally came to the conclusion that the router went bad. I got two more routers and they were both DOA, dead on arrival. I've gotten a third one, which is sitting in a box; I got it

Friday. Because I want to go very carefully when I implement it because temporarily, I've got it running off my wifi router and a lot of my components aren't compatible with a wifi router, either wired or over wifi. We've got enough; I've got a printer running, etcetera, etcetera. For instance, I can't scan right now so it's going to take a little while before [pause]

Yost: Sure.

Johnston: Just like I uploaded that rather large pdf for you, what I think I'm going to do is from now on, I'm going to upload to that particular directory and just let you know there's more to play with. I think it makes more sense than sending stuff by e-mail. If I convert this into a pdf, it definitely won't go through. In fact, I had — what the hell was it? — I had something for somebody else; oh, I know; I mentioned photography, right?

Yost: Right.

Johnston: I am a lover of photography to this day. And I've got some friends who are real good at it 'cause we're trying to solve a problem for me, but that's about buying another camera and I've got too many cameras now. My second cousin and her husband starred in a play at a local theater for six weeks. I got a front row seat and I shot that thing from start to finish; possibly one of the best photographic efforts I've ever made. And I didn't have her e-mail address or her phone number; and for whatever reason, her brother wouldn't call me back. So this past Saturday, her husband was starring in a one-

performance play, I said she'll be there. And she was there. I caught her; I told her; but again, it was too big to e-mail. So I uploaded it and told her to call me if she doesn't know how to download it. It's so easy; the URL just takes you right there. But that gave me great pleasure to see her; I hadn't seen her in quite a while except when she's on the stage.

Yost: Well thanks so much. This has been tremendously helpful and we're really glad that you're going to be at our workshop in July 2014.

Johnston: That's kind of exciting for me. Your presentation period is rather short; I understand why you have to do that.

Yost: It's geared towards more discussion time, everything being pre-circulated, to improve the papers for publication.

Johnston: Okay.

Yost: Great. Thanks again.