

## IR PODCAST

# IBM AND THE FUTURE OF CRIME

JANUARY 20, 2006

To hear this podcast and others from IBM, please visit [www.ibm.com/investor](http://www.ibm.com/investor).

**The first years of the 21st century have witnessed a watershed in the nature of crime. For most people, the threat of cybercrime is more real and more urgent than the risk of physical crime. Management priorities, crime-fighting resources, investment and education are at the start of a rapid adjustment.**

EDWARDS: I'm Ben Edwards. The early years of the 21st century are witnessing a watershed in the nature of crime. In rich countries, physical crime rates continue to decline.

Meanwhile, cyber crime is exploding in importance. For the majority of us, the threat of attack on our identities, our data and our online business activities has become more real and more of a worry that the threat of physical crime.

Behind this watershed lies not just the frequency of cyber crime attacks or the growing importance in our lives of online communications and commerce, but the changing nature of the cyber criminal himself.

Once the domain of amateur hackers and misguided pranksters, cyber crime today is characterized by elaborate profit-driven schemes involving organized crime syndicates. With me today to help explain how we adjust and adapt to this new and unfamiliar future of crime are two experts on cyber crime and security: Dr. Charles Palmer and Bob Bragdon.

Charles leads security and privacy for IBM Research; Bob is publisher of CSO magazine. Bob and Charles, welcome to this IBM podcast on the Future of Crime.

PALMER: Thank you.

BRAGDON: Thanks.

EDWARDS: Over the last few years I've noticed that I as a consumer and as a layperson have been paying more and more attention to security, security of my data. But at the same time I kind of feel less secure and more at risk. and there's more of a worry. In other words, I don't feel

like I'm getting anywhere in tackling that problem. Is that...you know, am I atypical, or is that a...you know, a common phenomenon, or a general phenomenon?

PALMER: I think you're very typical. The frustration that everybody feels is the, gee, I want to use this new medium because of the value it brings, this new technology. And yet it doesn't come without its sticky points.

You know, it's...it's.... I've always said, when hackers attack machines, it's because they can. In the good old days they did it for grins and for hacker points amongst their friends, and now it's actually for fun and profit.

EDWARDS: That point about, you know, the changing nature of the perpetrator. Just explain to me a little bit more about, you know, how that's evolved.

PALMER: Well, what we have seen over the last 10 years at least that I've been really into this, it's a move from [this what we call the] script kiddie, the little guys and gals who download something, gee, I wonder what this does, and...

EDWARDS: This is the script kiddie?

PALMER: Yes, someone who downloads a script of commands, tries it. And it's gone completely from those days where they might not even know what kind of machine you're attacking, [but] run a UNIX script against a Windows machine and then wonder why nothing really works.

It's evolved from, shall we say the novice, to much more of a pro. The person knows what they're after, they know how to get it. And there's very little fooling around. And you're much less likely to know they're doing it.

EDWARDS: So more sophisticated and committed by professional criminals, Bob. Is that...

BRAGDON: Yes.

EDWARDS: Is that the right [INAUDIBLE]?

BRAGDON: Absolutely. It is...it is shifted dramatically because it is being driven by

money. We saw a dramatic shift probably about two years ago in some of the research we did where we saw it, to Charles' point, it wasn't so much the script kiddies kind of out there...

EDWARDS: Okay, right.

Do we know...do we know who these professional criminals are? Do we have a good sense of who they are, and...?

BRAGDON: A lot of them are eastern European organized crime, quite a bit of it. But there are people in Iowa doing this as well. There was a recent case not too long ago where a number of individuals in Iowa pleaded guilty to breaking into a database, stealing identities and then trying to sell them.

EDWARDS: So, I mean, is there kind of a technical barrier to committing this crime? And you were talking about script kiddies before; the image I had in my head was, you know, of an adolescent boy but who had kind of gifted computer skills and could therefore do this. I mean, do you need technical skills to be able to accomplish this crime?

PALMER: Well, one point I want to make is this is an equal opportunity area.

[LAUGHTER]

Whenever you say.... Typically you think it's this teenaged guy, overweight, with a...

EDWARDS: Right.

PALMER: ...[INAUDIBLE] [soda pop].

Our experience was that there may not be as many women in it, but there certainly are. And the advantage that they have is that there are so few in it that they have...there's less suspicion applied to them when they are...

EDWARDS: Interesting, yes.

BRAGDON: We've trained our populous so well in computer technology that they're...a lot

of them are coming back and using it against us now unfortunately. There are Web site out there that have all the tools you need to use that you can just download and crack into, you know, a SQL database or whatever.

And it doesn't take a tremendous amount of knowledge to be able to do it. To get in the more sophisticated types of attacks launching distributed denial of service attacks for extortion purposes, for launching kind of wide scale phishing attacks; that gets into something a little bit more complicated.

EDWARDS: Right.

Now, you've mentioned a few kind of variety of attacks and so on and so forth: phishing, and denial of service. Just takes us through a couple of the important ones and you know, and what they do and what sort of threats they pose. And you know, why it's important that we, you know, try and prevent these things happening.

PALMER: Well, one of the oldest ones of those you mentioned is the simple denial of service, where you simply...it's sort of what happens every year on Mother's Day when you try to call mom...

[LAUGHTER]

...there's not enough circuits, right?

Well, every computer has only so much capacity to communicate. And if I can do something to sort of tie up that capacity, then you're off the Net.

And now it's gone from, that was a very high-profile target to the last one I heard about was a t-shirt company in New Jersey, had put up a Web site, and one of their competitors that was bigger than they were was -- "suspected," of course -- of leading the assault on their Web site. And they called us to try to get some help, and we just said, there's these FBI guys you should call.

[LAUGHTER]

EDWARDS: I see.

BRAGDON: And I'll tell you, distributed denial of service attacks have gone to kind of the next level too. Last May in CSO magazine we profiled an extortion case of an offshore gambling company, offshore gaming company, who had had a denial of service attack launched against them.

Someone had broken into their system, been able to access some of their data, turned around, launched a...basically took the Web site down for a few hours and then sent them an e-mail saying, send us \$50,000.

They were unusual in that they fought it. They spent over a month fighting this. They brought in outside experts. They ended up.... They figure the whole thing cost them well over a million dollars over the course of that little over a month.

EDWARDS: Wow.

BRAGDON: But ultimately they fought off the denial of service attack that basically was taking them down on big weekends like the Superbowl [CHUCKLES] weekend, and...

EDWARDS: Right, right.

BRAGDON: ... things like that, where all their business was generated.

EDWARDS: Okay.

PALMER: But then there's the more recent one of phishing, and this is [what's]...we all get e-mail that says, your Paypal account needs updating, or your this, or your that. Click here and go there.

And what the bad guys are doing is they're hiding a naughty Web site behind the words saying the good Web site.

EDWARDS: I see.

PALMER: I mean, it all comes down to trust. To use that old thing everybody's heard about on the Internet, nobody knows you're a dog. Well, that's part of the problem, because originally it was a feature, and now it's a bit of an issue because we're trying to establish trust with basically strangers. Trust among strangers is really what we want to do now.

EDWARDS: Right.

EDWARDS: Do we have a good handle, Bob, on how prevalent this is?

BRAGDON: Well, it's like spam, everybody gets it at some point.

EDWARDS: Right.

BRAGDON: It just depends on how much you get and whether you actually take advantage of it or not. We every year conducted a study with the US Secret Service and [kind of e-mail insert] on electronic crime and cyber crime. And two years ago, phishing wasn't even on the radar. Last year it was second most prevalent crime.

EDWARDS: Right.

BRAGDON: It...it has just exploded

EDWARDS: And circle back to this, you know, the way we began this, with my sense of frustration that we're not [getting it], why is it such a difficult problem?

PALMER: My big complaint, or my, one of the research areas that we drive is security by design, security engineering. It's kind of like the airbag in your car.

EDWARDS: Yes.

PALMER: If you don't have one in your car it's really going to be kind of weird if you install it yourself: are you really going to feel safe? Or would you rather have it done at the factory?

EDWARDS: Yes.

PALMER: The same thing is true about computer systems. They should be secure by design from the beginning, and that's what people are beginning to realize, and that's where we have to go.

EDWARDS: So in other words, instead of bolting it on, you have to build it in from the beginning...

PALMER: Right. Right.

EDWARDS: ... in how you structure the architecture and put it all together and...

PALMER: Exactly. That's one of the reasons security is such a pain in the neck.

I mean, at last count I had 93 passwords. Obviously I don't keep them all in my head, and they're not all the same, which would be a bad thing. But there's got to be a better way to do that, and whether it's a biometric, one of many different choices, or some other kind of identification system, we have to [make] some example of how we're going to make security a lot easier.

EDWARDS: So where do you keep your passwords, Charles?

PALMER: Why should I tell you?

[LAUGHTER]

BRAGDON: A Post-It on the side of the monitor.

PALMER: We actually did ethical hacks where the guy had 15 different little Post-Its on his monitor.

[LAUGHTER]

And I asked him, sir, don't you think that's not terribly secure? And he said, well, you don't know which one is active, because he never took them down, he just moved...

EDWARDS: Ah!

[LAUGHTER]

But still only 15 choices.

[LAUGHTER]

PALMER: Right.

EDWARDS: Yes. So this, clearly this identity question is troubling, right? Because...!

mean, is there an elegant solution to that, to the...you know, so that I don't have to, you know, have a billion schemes, so that you know who I am and I know who you are?

PALMER: Part of the problem is establishing that trust, and what sort of credential we can use. Biometrics are very appealing; they are not without their risk and they are not in some cases as good as you might think they are. Not everybody has a fingerprint...

EDWARDS: Is that right?

PALMER: Oh, yes. There's a small percentage of the population for which that doesn't really work.

EDWARDS: Interesting.

BRAGDON: But there are a lot of competing solutions and technologies out there, and I think that's part of the problem, is that there are so many, and there are so many bright people out there that have developed so many different ways of trying to establish some level of that trust that there's still a certain amount of wash out that's going to be happening in the marketplace before we start to settle down into kind of one, or two, or three different families of technologies and approaches that will...that will work for a large percentage of cases.

PALMER: What we've certainly seen is since 9/11 in particular everybody and their brother is now a security consultant.

EDWARDS: Yes.

PALMER: You know, guards, gates and guns, physical stuff to cyber this, to [million bit crypto] algorithms.

EDWARDS: Right.

PALMER: We get to examine a lot of those opportunities for our customers, and it's always entertaining.

[LAUGHTER]

And there are new technologies, and you don't want to miss one, it might be the best thing since

canned beer. But then again, if it's a million bit crypto kind of thing you just kind of...

BRAGDON: I want to, if I could, just step back a second and share one story with you, just to kind of put the whole identity theft issue in context. You may or may not be familiar with the [shadow crew] case that the Secret Service broke about a year and a half ago where they had executed a warrant in New Jersey for identity theft, gone and found that this individual was actually basically the webmaster for this [shadow crew] Web site, where...which was a clearinghouse for identities, stolen identities, worldwide.

And there were hundreds of thousands of identities being traded through, being sold through this Web site. They were actually raided based upon the credit limits that they could get. You would pay \$40 for a good identity with a high credit limit or you pay \$20 for one that only had a thousand...a thousand dollar credit limit.

Secret Service took this over and ran it for six months and actually advanced the site to the point they would put in...they put in a VPN, a Virtual Private Network, so that the identity thieves, once they created accounts and credit cards, could check them before they went into the store to make sure that they were still valid.

So they'd sit in their car, they'd run it through...over the VPN over a wireless network, run it for a dollar to make sure it was going to go through and then they'd go in the store and they'd ring up \$500 and [then go up].

And it was all bogus, it was all set up by the Secret Service, and they ultimately brought down people in quite a few countries when they broke this down. It was, that's organized crime at it's...at it's...you know, most scariest I guess is the word I'm searching for.

EDWARDS: Yes.

BRAGDON: It is very sophisticated, and they're using very advanced technology to do real basic things.

PALMER: But it wasn't just credit cards. A lot of people, when they hear identity theft, they think, oh, they got my credit card number. It's a lot more than that. And I have screenshots from that...that gig, shall we say...

[LAUGHTER]

Where not only, I mean, 50 bucks for a working credit card with some limit, but if it was a much more complete personal record: mother's maiden name, home addresses back three years, whatever, you know, you got a lot of money for that, too. That was like 250, 300, 400, for more personal information.

EDWARDS:           What can I do with that extra level of personal information that they can't do with just like a credit card number and account?

PALMER:           Well, you could open another credit card number. You could open another credit card.

EDWARDS:           Right.

PALMER:           And open a bank account.

EDWARDS:           Right.

PALMER:           You could open up an eBay, Paypal, Amazon...

BRAGDON:           Bank loans.

PALMER:           Oh, yes.

BRAGDON:           Yes, I mean, that's when you start getting into huge, huge amounts of money.

PALMER:           And you can also get into huge, huge kinds of harassment where an early security consultant went on a trip and he came back and found his wife had been served with divorce papers.

EDWARDS:           Wow.

[LAUGHTER]

PALMER:           So he had just, you know, put one guy too many out of business.

[LAUGHTER]

EDWARDS: They must have really worked on that scheme.

[LAUGHTER]

Extraordinary.

EDWARDS: So as one final question. I mean, we started this conversation with the notion that you know, cyber crime is becoming more prevalent, more important to our lives than physical crime. And do you think that people actually feel that and businesses feel that?

BRAGDON: I certainly see that. I've seen a big jump up. I think part of it is an awareness issue. We had a lot of data breaches earlier in 2005, and that really raised awareness for the average person on the street of what the issue was. And so it's being addressed, you know, at a much higher level now.

PALMER: Yes, I would agree that there's no doubt that this is going to continue to happen. It's even a measure...been measurable through surveys on the activity on the Web as far as e-commerce.

EDWARDS: Right.

PALMER: I think just a few percentage points, not a lot, but a few people have actually said, you know, I'm going to cut back on this because I'm just worried.

EDWARDS: Right, so it's beginning to bite.

PALMER: Yes. I mean, my dad just has still refused to ever buy anything on the Internet even though, you know, I tell him how to do it. You'd think he'd listen to me but...

[LAUGHTER]

...never has.

EDWARDS: Well, some fascinating thoughts there. Bob Bragdon and Charles Palmer,



thank you very much for being with us today. This has been an IBM podcast.

PALMER: Thank you.

[END OF SEGMENT]