

Insider Threats – an Interview with Bill Crowell – Former Deputy Director of the NSA

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining us today is Bill Crowell. Bill is a security expert and long-time friend. I'm extremely happy to have him on today's podcast. Bill is an independent consultant on areas of information technology, security, and intelligent systems and serves chairman of the senior advisory group to the Director of National Intelligence.

He also served as president and chief executive officer of Cylink Corporation from 1998 until its acquisition by SafeNet in February 2003. Bill also worked at the National Security Agency for several decades where he held a series of senior executive positions such as Deputy Director of Operations and Deputy Director of The NSA. He also serves as director of several private companies.

Bill has been quoted in many trade and business publications including the "Wall Street Journal," "Business Week," and "USA Today" and is coauthor of the book, "[Physical and Logical Security Convergence](#)".

Welcome to the show Bill.

Bill Crowell: It's good to be here again with you, Brian.

Brian Contos: Bill, you live a fascinating life. What's the latest and greatest that you've been involved in?

Bill Crowell: Well, it's interesting. I've been expanding my horizons to include working in the area of computer forensics and attack forensics lately. It's been very interesting for me having been an attacker before. It's very interesting to see what the new tools are for discovering how an attack place.

And of course, forensics is very important because the whole insider issue. Without good forensics, you can't really establish who did what and be able to deal with it, whether it's in an HR sense or a prosecution sense. So that's a fascinating new thing that I'm doing.

I'm working on a number of projects for the government as well that are important and interesting for me. I like to stay engaged with my former colleagues so that I can help every once in a while bring old thoughts to new problems.

Brian Contos: Very cool. We've known each other for a number of years now and we've discussed insiders more often than I can count. One of the things that I can recall you

Insider Threats with Former Deputy Director of the NSA Bill Crowell

saying to me about a year ago was that the term "insider," in and of itself, was starting to lose meaning. Do you still feel that way? And if so, can you elaborate on what you mean by the term "insider" losing its meaning?

Bill Crowell: Well, I still feel that way. I guess I feel that way even more now for some pretty new reasons. First of all, I think that we have over the last couple of years seen examples of where the number of remote attacks has been increasing considerably.

Their potential success has certainly increased of late, partly because of supply chain issues. From what I would call enablement of these attacks by mistakes, flaws, or induced flaws in various products just because of the general nature of the Internet.

We essentially have an Internet that enables connectedness. So if you are able to penetrate the perimeter of defenses, essentially, you are an insider, for all practical purposes, on someone's network.

Brian Contos: If you take into consideration how much information is digital and how connected we are today, it's pretty straightforward to say when everyone's an insider, nobody's an insider.

It's definitely interesting. I've talked to a number of organizations that have very complex SOA architectures, they've got customer service portals, everything from checking your healthcare records to your academic records, and your financial information from your computer or your mobile phone. It's all interconnected. There's just a massive amount of information out there that's made readily available. Of course that introduces those risks.

Bill Crowell: Years ago, there was a "New Yorker" cartoon that had two Dalmatians sitting in front of computers. And one said to the other, "On the Internet, everyone's a dog". I think today, on the Internet, everyone's an insider. There are no perfect perimeter defenses. We have under-deployed authentication, have allowed people to have complete access to everything once they're inside a network.

So we've created an opportunity for both the true insider and the remote access user to pretty much have total access once they've penetrated.

Brian Contos: Bill, you're in a very unique position in that you've been CEO of a publicly traded Silicon Valley Security company. You have several decades with the NSA and even longer working with the federal government as well as being a consultant for many, many organizations. Is the government's approach to insiders different than that of what we see in the private sector?

Bill Crowell: Well, unfortunately, there is a difference between the government's approach to insider threats and that of most of the industries I'm associated with. I guess the best way to illustrate that is that the financial industry has a lot to lose to any insider gaining access to intellectual property, to financial records, to actual financial resources like money transfer systems and the like.

So they take the issue of insider attacks and fraud in particular -- they refer to it as fraud -- they take all of that very, very seriously and they have very elaborate systems, both manual and automatic, that cross check what individuals within their networks are doing.

For example, they have legal requirements to prevent someone who's working on M&A kinds of activities from talking to other people in the company who are doing analysis or

analyzing company performance. A lot of these have grown up over the years because there have been real fraud committed across these various business areas.

The government tends not to treat the insider quite the same way. I remember, for example, one case of espionage. The government actually had to put a camera on the ceiling, staring at the screen of an individual in order to know what they were even looking at, because in their classified networks, they did not have adequate logging and authentication and all of the kinds of things we see deployed in the financial industry that would make it possible to, from a forensic standpoint, prove that someone had access to a particular document.

And so, while I think that is about to change -- in fact, I'm pretty certain that's about to change -- there is less history in the federal government of tracking what individuals are doing with applications and with databases, making that information correlate-able and track-able.

Brian Contos: Bill, there's so many statistics out there on insider threats from studies done by CERT, Carnegie Mellon, the FBI, Secret Service, there's even certain organizations like Verizon, that have released research documents that have some pretty compelling evidence around insiders.

But they're all predicated on the fact that these are insiders that have actually been detected and are caught. What do you feel is the most under-reported aspect of insider threats?

Bill Crowell: Well, the magnitude of some of the losses are certainly under-reported, and probably for good but not sufficient reasons. I say good reasons, because a lot of institutions that have reported what their losses were, have been punished for it, either in the marketplace by their competitors, or in some cases, by prosecution or other enforcement or regulations, like Sarbanes-Oxley, and so on.

There are not a lot of reasons for people to report the magnitude of the losses. Again, what I'm seeing in this whole world of cyber attacks is that, increasingly, cyber crime is a rewarding endeavor.

And it's rewarding in the sense that the attack can be monetized, and therefore, it's like any other economic crime, like robbery. It's also rewarding in that there are fewer consequences, whether you are talking about it in terms of incarceration and prosecution, or you're talking about the likelihood of even being tracked at all.

Brian Contos: Yeah, that makes me think of two things. The first is a quote from G. Gordon Liddy, where he once said, "If crime didn't pay, there wouldn't be crime."

Then at Black Hat in Las Vegas this year, I was watching a presentation about Russian cyber criminals. In particular there was this one that was in prison for committing multiple instances of cyber crime. And he was serving a fairly short term. The reporter asked him -- they said, "What are you going to do when you get out of prison?"

He said, "I'm going to do exactly what I was doing before I got put in, which is cyber crime." He said, "I have made more money in a year than I could ever make."

He goes, "I could retire, my kids can retire, and their grandchildren can retire." He goes, "There's so much money to be made, the reward is so high, and the risk is so low. Why would I want to do anything else?"

Bill Crowell: Well, and as we've all experienced throughout history, crime is only diminished when there is some reasonableness to the expectation of being caught. Deterrents work. They may not work perfectly.

There are some people who will take more risks than others, and there are some people who think the reward is such that they'll take any risk, but in terms of the magnitude of the threats that are out there today, I think they are encouraged by the lack of enforcement and the lack of tools for finding the insiders when they perpetrate crimes.

Brian Contos: And Bill, building from a statement you just made a few moments ago about disclosure - is there really any advantage for this organization to report the magnitude of its loss.

When we think about disclosure laws which are now in 40 plus states, like California Senate Bill 1386, and you look at the fact that if an organization gets hacked into, and let's say they've got a million users on this database, and they don't have the forensics ability to really analyze the extent of that threat, they pretty much have to assume that all those individuals were compromised.

And then you get one of those letters that says that your information may or may not have been compromised. Having the right tools to look into what was the extent of the breach -- perhaps they only accessed one table, and that table contained information on 100 users, instead of a million users. Well, that really helps mitigate the risk.

And I'll have to say this, sort of getting into a little bit more of a technical discussion, do you think when organizations are talking about protecting sensitive data, they're too focused on the file server and unstructured data in terms of documents and things like that, and they're not really paying enough attention to the structured data, and that is all the sensitive data that resides in these very complex databases?

Bill Crowell: Oh, absolutely. And I'll make another point that's related to this as well. If you look at the way we store data today, we store very, very sensitive data all together, which makes it even more sensitive.

There are tools out there today that would allow you to split knowledge, or to hide information, in tables that you can control access to, in much better ways. For example, it's perfectly reasonable to build a database in which Social Security numbers are hashed, but you still have the ability to compare activities of the person by Social Security number because you can compare their hashes, but you aren't revealing the Social Security number to all the users of that database.

I think what's happening today in regard to improving security, is that people are beginning to understand that it's not just the perimeter. Or as we said in our book, "It's not the moat." Our layered defenses and that many of the defenses have to be on the inside of the network in the applications or in the databases, if we really want to protect information.

Brian Contos: Absolutely, and to just put a little plug in there for the book Bill mentioned, it's called ["Physical and Logical Security Convergence."](#) and the two of us, with two other gentlemen, Dan Dunkel and Colby DeRodeff, wrote this book.

That actually takes me to this next logical point: sensitive data. We understand that clearly is the target. That's what the bad guys want. Credit card information, PII, intellectual property, and other sensitive data is in fact the "crown jewels."

Insider Threats with Former Deputy Director of the NSA Bill Crowell

And we understand that sensitive data resides on databases, and bad guys generally get to databases through web applications, both internal and external, or through direct access.

But doesn't prudence then dictate that that's where we put most of our security controls? We really focus on protecting the data at the application and the database layer, but I really feel, and let me know what your experience is, that data security is almost where network security was in the mid- to late 1990s and we certainly have a lot of catch-up to play.

And it's almost like, to continue to mix metaphors here, it's almost like it's the Wild West when it comes to data security, where network security, perimeter security, I think is, well, not perfect, has really gotten to a really stable point. Do you feel that way, too? Do you feel we're a little bit behind?

Bill Crowell: Well, I do feel that we're behind, but I'd like to inject kind of quickly, lest we suggest to people that they concentrate on the new area at the expense of old areas, that I'm a great believer that we need to have security systems that are highly integrated, and that do in fact attach themselves to all of the places in which people might be able to penetrate and achieve access to sensitive data.

So we can't forget the perimeter, it's still important. We haven't done enough at the perimeter, like authentication, and identity management, but we also haven't done nearly enough in databases and applications security.

And so we've created this additional set of vulnerabilities for insiders, for remote access using insider knowledge or insider access, and for supply chain induced problems, such as those that we see at operating systems and applications that are being written offshore, and so on.

And we have to address all of those in order to be able to someday say that we have taken all reasonable measures to protect sensitive data.

Brian Contos: Well, Bill, we just about time for one more question, but you know me, it's one question, but I'll do it in three parts. [Laughs]. In terms of insider attacks and the future, who's going to be the target, what's going to be targeted? How do you think this information is going to be leveraged?

Bill Crowell: Well, I was talking to the former acting White House advisor on cyber security a little while ago, and her name is Melissa Hathaway. And Melissa has the compassion, and I agree with her, about essentially the carnage, raping of America's industrial base.

It essentially boils down to the fact that the thing that distinguishes us as a nation is our ability to innovate and create, and to do that very rapidly and move very rapidly and stay ahead of our competitors, and yes, our enemies as well.

And I think what we stand to lose in this whole game if we don't begin deploying better solutions, is that corporate America, companies that distinguish this country, will be so penetrated that we will begin losing our competitive advantage internationally. That's scary to me.

And I believe that that's something we all should be worried about, and that's the reason that security is a profession that really needs to step up to the table and begin integrating across all the solutions faced rather than just producing point solutions.

Brian Contos: And Bill, one thing to expand on that message, and one thing I tell all people out in the field is, that if you look at an external attacker, whether it's some type of nation-state threat, organized cyber criminals, you know, some portion of the RBN, the Russian Business Network, or perhaps even a terrorist organization, they're going to look at the ROI (Return on Investment) of trying to hack into your organization.

And certainly there's those groups that are going to try to hack in from the outside, because as you mentioned, Bill, the risk is low, the reward is high. But also, if they really empirically need to get that information, they'll likely resort to more traditional measures: blackmail, extortion, bribery, things like that.

Why hack, when you can recruit? You can leverage an insider that's sympathetic to your cause, has something that you can hold against them, such as a gambling debt, or drug addiction, or whatever the case might be.

Maybe their house is being foreclosed on and they're going into bankruptcy. Who knows? And you need them to download information that they have access to every day. It's very easy to do that.

And one of the cases that always comes to my mind when I start thinking about this is Ellery Systems in Boulder, Colorado, and this was actually one of the things that led to the 1996 Economic Espionage Act. There was a Chinese national who was working as a programmer, and he stole the intellectual property, source code, from Ellery Systems, and gave it to a direct competitor called Beijing Machinery in Beijing, China.

Ultimately, when they competed for business, Beijing Machinery was able to undercut the cost because they didn't spend any money on research and development, just on sales and marketing. Subsequently, Ellery Systems went completely out of business. The company died.

Again, that's a little bit of early history, but it did lead to the Economic Espionage Act and I think it's a great example of just what level of damage that these types of things can cause, to put an entire company out of business. Had it been very, very sensitive information, it could have put a lot of people at risk, as well.

Bill Crowell: Well, I'll make one closing remark with regard to insiders. In today's world, it is quite possible to recruit and use an insider without them even being aware.

I mean, the level of bad practices that go on within companies and the use of their networks is just really astounding. For example, I have in my pocket right now a USB token. It was given to me this afternoon. It has a huge amount of intellectual property on it.

And at the same time this was being given to me, so that I can work on some information, I have no idea where this USB fob came from. And I have read about picture frames and all kinds of things being used as Trojans for gaining access for information, so am I going to become an insider when I actually put this on my computer?

And then give it back to them with the corrections and changes, who has augmented an attack? I really don't have any way of knowing. And so, we have to identify ways in which people can be unwittingly made insider augmenters to outsider attacks.

Brian Contos: Very well stated. Well, Bill, thank you so much for joining us on today's podcast. I think this was an incredible insight into this very important subject, and there's

Insider Threats with Former Deputy Director of the NSA Bill Crowell

very few people I know of that really understand insider threat as well as you do. So thanks again for joining us today.

Bill Crowell: Thank you Brian. Good talking to you.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200