

# Interview

## Silver Bullet Talks with Jon Swartz

GARY MCGRAW  
Cigital

Jon Swartz is a reporter for *USA Today*, covering computer security and technology. He has spent 20 years reporting for *Communications Week*, *Mac Week*, *Mac User UK*, and the *San Francisco Chronicle*. With Byron Acohido, Swartz wrote *Zero Day Threat* (Union Square Press, 2008). In 1997, Swartz was nominated for the Pulitzer Prize for his coverage of the Internet.

Featured here is an excerpt adapted from a full interview between Swartz and Silver Bullet host Gary McGraw. Their conversation ranged widely, from ID theft to cybercrime. You can listen to the podcast in its entirety at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet/](http://www.cigital.com/silverbullet/); you can also subscribe to the full series on iTunes.

**Gary McGraw:** You file about three stories a week. Do you ever feel like you're repeating yourself, or are things evolving so fast on the tech front that it stays interesting?

**Jon Swartz:** I think you're right on both counts. On one hand, it's always new, especially security—it's always evolving. For instance, we wrote a book called *Zero Day Threat*, but now I'm hearing of something called a "minus day threat," which

I'm trying to figure out.

On the flip side, it does feel sometimes like déjà vu or *Groundhog Day* when you're working at a newspaper. It seems as if sometimes you're writing the same story over and over. That's one of the edicts in the newspaper business—you have to assume that no one has read your story before, so you have to trot out some of the same material or recast it at times.

**McGraw:** After a decade of covering this space, do you think global business is doing enough to manage security risks?

**Swartz:** In some cases, it is; but for the most part, no. What is kind of galling is that during the process of researching and writing this book we came across this consistent mantra that the consumer is somehow to blame for making silly mistakes. Whether it's security or airlines or insurance companies, the onus is always put on the poor consumer who's at the end of the food chain rather than on security that should be there in the first place.

We're trying to be a watchdog in some cases, but sometimes it's hard to cut through the clutter. There was this big hue and cry when debit-card information for members of the Senate went missing. There was a lot of saber rattling from Washington D.C. about some form of legislation.

Well, it turns out they lost interest in the topic because John Roberts was being considered for the [US] Supreme Court and [that] shifted their interest.

Since then, we've seen the TJX [parent company of TJ Maxx and Marshalls] breach. I'm almost convinced that there is actually a breach that's going on now. Maybe it's not as big as TJX, but it's probably on par and we probably won't hear about it for several months.

It's crazy. When we talk about ID theft and all this vast amount of digital information out there—when it does end up in the wrong hands, everyone just thinks that they're going use our credit-card numbers and maybe create fake identities to sell to other people. But increasingly, I'm hearing from people in the state department that there is a real concern that some of that information might end up being used to create fake passports for people to cross into the United States.

**McGraw:** What is *Zero Day Threat's* take-home message?

**Swartz:** There's several things. First, what we want to do is explain to people how all this cybercrime and ID theft, all these stories that they read about, how they all kind of fit together. For instance, how hacking evolved from a hobbyist activity to a for-profit motive, going back to the Sasser worm.

## About Jon Swartz



Swartz has a BA in journalism from San Jose State.

**U**S *A Today* reporter Jon Swartz has spent nearly two decades reporting on technology topics, dating back to his days at *Communications Week* and *Mac Week* where he regularly broke stories on turmoil within Apple Computers' executive ranks. In 1997, Swartz was nominated for the Pulitzer Prize in Beat Reporting for his Internet coverage while working at *The San Francisco Chronicle*. And in 2005, Swartz, with Byron Acohido, was a finalist for the Loeb Award. He is the coauthor of *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money*

What we also want to do is point out that banks, merchants, media companies, and tech companies are completely committed to porting commerce wholesale to the Net, yet the Internet was never intended to be a secure transactions network. The more deeply corporate America embraces Web 2.0, the more doors and windows it's opening for very focused profit-minded crime groups to exploit.

**McGraw:** Did you meet some of these criminals?

**Swartz:** I would communicate with them, sure. Some of them, including the guy who was the mule of the group in Florida, was talking to me off and on from prison. His name is Irving Escobar. The Florida case is interesting because it runs the gamut of how these operations work.

You have the guys on the ground level who have no idea who they're working with. Somehow, they get recruited to cash out after a series of transactions from the actual theft of the data, down to the people on the street who use the credit-card numbers to purchase gift cards from the Wal-Marts in Florida. I would go to the stores where these guys would ring up US\$20,000.00. They bought gift cards and merchandise worth probably about \$2 million, and that's a conservative estimate. The prosecutors told me it was much

higher, but they prosecuted their case based on the most easily prosecutable information.

What was amazing to me, though, was that I would call the victims, the credit-card holders, whose information had been breached and invariably, they were retired people in Southern California who'd never shopped at Wal-Mart and, in some cases, had never been to Florida. So, to me, this screamed out how in the world did this happen? Why wasn't this picked up by Visa or Bank of America whose credit-card numbers were being exploited? I mean, people had \$20,000 charged to their credit card in one day from one location.

**McGraw:** I also think that we're at this interesting point in history. If you look at reporting from when the telephone was first introduced, you would see stories about "telephone murder" or "telephone bank robbery," which just meant that somebody had used the telephone as a tool during the murder, maybe to call the victim and have them come over. I think there's a little bit of that effect these days too because crime has always been with us and the Internet just happens to be the tool of the day.

**Swartz:** One of the goals of our book is to show how the cybercrime economy is driven by capitalist principles and entrepreneurship. If you look at what

happened with TJX or even with ChoicePoint, you basically have these enterprising criminals who delegate tasks and authority among one another. They come together, they start basically a startup, and they disband when the heat really picks up. ShadowCrew [an international message board offering stolen personal information], I guess, had several thousand people involved, although only a handful were prosecuted. After that was busted up, you saw 12 iterations of ShadowCrew surface.

**McGraw:** Despite a string of highly publicized breaches at TJX and the Veterans Administration [US Department of Veteran Affairs], why does the general public have such a lax attitude towards computer security?

**Swartz:** Almost with every topic—and I hate to sound as if I'm speaking on behalf of the American public—but until somebody's victimized, it's just out of sight, out of mind. It's amazing. If spam wasn't effective, or phishing wasn't effective, we still wouldn't be seeing it in record numbers.

There's not enough education of the public. Sometimes you wonder if you have to educate the public in the way that, say, the auto industry was educated by Ralph Nader. I think Richard Clark has tried, but to a lesser extent. His focus is a little bit more on national security.

I think Gates was engaged for a while, but once he decided to shift into philanthropy, I think he lost interest or he just had to change his focus. I think it's a noble focus that he shifted to. I give him all the credit in the world. But I don't really think there's a central figure. I think when we see some of the CEOs, or hear from some of the CEOs of security companies, many of them speak in platitudes.

**McGraw:** Those guys don't understand the software security problem, frankly.

**Swartz:** They're several layers removed from what's happening on the ground level. It's almost preferred to talk to the engineers and those people.

**McGraw:** What can we do to boil down software security messaging enough to get normal people to understand it? That's, to some extent, your job.

**Swartz:** Well, that's what I'm hoping the book does. I hope it reaches a wide enough audience to do that. We've been doing a lot of radio interviews. You know what? I do give listeners on radio stations, in particular, credit. I was on a local radio show in San Francisco for about an hour, and got tons of calls. Almost everyone who called in was aware of security in way or another and they knew they had to update their antivirus programs or they needed a firewall. They knew they had to be paranoid about email attachments and wouldn't open them unless they were absolutely certain that they were legitimate. A lot of them weren't aware of some of the new vectors such as their own Facebook profiles, which is a little terrifying.

**McGraw:** How about the online game stuff?

**Swartz:** Yes, that's another one. A lot of them mentioned that. In a sense, it's filtering out. But again, it still astounds me given the breadth of coverage how it tends to be overlooked. One of the things we decided to do with this book is write a tech-crime thriller type of book.

We're approaching this like the movie *Traffic*. You have multiple narratives of a problem. There is a parallel between this and the drug industry in that if it doesn't touch

you directly, it's kind of out of sight, out of mind. Or like the environment. Everyone talks about the carbon footprint. We were trying to establish some idea of a "digital footprint" before it really has major implications, if not already, on economic systems or people's trust in shopping and searching online.

I really don't know how you can really resonate with the wide stream public unless there is some sort of incredible event that takes place.

**McGraw:** Even then it's tricky. I'm a computer scientist and a software security guy. Yet, when I go to a cocktail party at somebody's house, even pretty well-informed intellectuals go, "Oh, you're a computer guy. Can you help me with my home PC problem?" And I just sort of say, "That's not the kind of computer guy I am." That's the state of the real world out there.

**Swartz:** If I were a criminal, I couldn't think of a better crime to commit because it's basically free money. The infrastructure costs are minimal. There's no threat of violence.

**McGraw:** What is it that Dean Takahashi [*San Jose Mercury News*] said about cybercrime?

**Swartz:** He talked about *The Sopranos*. If they were getting into a new business, this would be it. Think about it, though. You have this arguably 200-billion-dollar-a-

But out in the deeper running water, you have the elite hackers trading 0-day viruses, running massive botnets like Storm, operating bulletproof hosting services like Russian Business Network. The big guys operate, as Dean Takahashi said, like Al Capone at the height of the prohibition. There's no Eliot Ness out on the horizon to slow them down as far as I can see. There was a bit of an effort within the FBI to make cybercrime a top priority. I don't think they had the resources, the people, or the know-how to make much of a dent. I wouldn't say that publicly, but I think privately, they would acknowledge it.

You can find additional podcasts in the series, including those featuring Mary Ann Davidson and Adam Shostack, at [www.computer.org/security/podcasts](http://www.computer.org/security/podcasts) or [www.cigital.com/silverbullet](http://www.cigital.com/silverbullet). □

**Gary McGraw** is *Cigital's* chief technology officer. His real-world experience is grounded in years of consulting with major corporations and software producers. McGraw is the author of *Exploiting Online Games* (Addison-Wesley, 2007), *Software Security: Building Security In* (Addison-Wesley, 2006), *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and five other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer sci-

**If I were a criminal, I couldn't think of a better crime to commit because it's basically free money. The infrastructure costs are minimal. There's no threat of violence.**

**—Jon Swartz**

year industry where you have script kiddies and novice scammers kind of splashing in the shallows, grabbing law enforcement attention.

ence and cognitive science from Indiana University. He is a member of the IEEE Computer Society Board of Governors. Contact him at [gem@cigital.com](mailto:gem@cigital.com).



**\$29**  
New Lower  
Subscription Price!

IEEE  
**SECURITY & PRIVACY**

Subscribe to our  
magazine today  
for only \$29—  
our lowest price ever!

You'll receive 6 issues of today's  
leading-edge, peer-reviewed  
software development information.

Ask us how  
you can get this great deal on  
*IEEE Security & Privacy* magazine!

*S&P* is the premier magazine  
for security professionals.  
Every issue is packed with  
tutorials, best practices, and  
expert commentary on:

- attack trends
- cybercrime
- security policies
- mobile and wireless issues
- digital rights management
- and much more.

Subscribe at [www.computer.org/services/nonmem/spbnr](http://www.computer.org/services/nonmem/spbnr)