IT Professional Offers Advice for Outsmarting Cyber Thieves
Greg Scott's Debut Novel Reveals the Anatomy of an Electronic Break-in

(Twin Cities, MN) – Target, Home Depot, T.J. Maxx, Sally Beauty Supply, and the list goes on.

Most Americans know what these companies, and many others, have in common. They have all been victims of cyber thieves—criminals who use the Internet to steal not just from the companies, but their customers as well.

According to Greg Scott, an IT professional and author of the novel, *Bullseye Breach: Anatomy of an Electronic Break-in* (Beaver's Pond Press, 2015, $18.95), most of the attacks could have, and should have been prevented. "I was outraged by the data breaches at Target and other companies," he says. "These huge breaches make me crazy because the so-called sophisticated attacks would never have happened if the right people had been on the ball."

Scott explains what happened at Target. "The Russians apparently gained access to the entire Target network by compromising the credentials of an outside vendor. Once inside, just like criminals inside a house searching for valuables, they systematically searched the Target network looking for valuables. They struck gold when they found thousands of Point of Sale (POS) systems across the United States to plunder."

Scott says the company's POS systems should have been behind an additional firewall. They weren't and that's why they were compromised.

After the Target breach happened, Scott, who has been working in the computer industry since the 1980s, felt compelled to write a book explaining what companies could do to prevent themselves from falling victim to cyber thieves. To offer examples of what could go wrong, he started working on some short stories to accompany the text. It wasn't long before those short stories took on a life of their own, eventually turning into a full-length novel.

Bullseye Breach: Anatomy of an Electronic Break-in is the story of how a major Midwestern retailer fell victim to cyber thieves from Russia. Throughout the book, the author offers specific details about how the attack was launched. First, the attackers probe widely across the Internet, looking for vulnerable targets of opportunity. After they find and penetrate Bullseye Stores, they probe the Bullseye network deeply to steal the key information they need to compromise thousands of POS systems and rob millions of customers. The Bullseye story is fiction. The tactics are very real.

Bullseye Breach

Greg Scott

Bullseye Breach
ANATOMY OF AN ELECTRONIC BREACH

Greg Scott

Feature Article

Shortly after the attack the story's hero, IT consultant Jerry Barkley, is called upon to track down what happened and install safeguards so it can never happen again. "I wrote the story in such a way that readers will be educated as they make their way through the story," says Scott, who adds that if he had been in charge of security at Bullseye Corp., or any of the real companies that have been targeted, he would have done exactly what his main character does in *Bullseye Breach.*

"If you're a retailer, you need to protect those Point of Sale systems by keeping them in their own private network. Put a firewall in front of them and use a whitelist to limit what those POS systems can access. If they try to go outside the whitelist, then notify the right people," says Scott.

Retailers running credit cards aren't the only types of businesses that need to protect themselves. Scott says it is critical for all organizations to protect their most private data. "It doesn't matter if they're politicians running for office and storing donor information, or if they store credit card information to sell hammers, or if they store sensitive medical data," says Scott. "When somebody wants me to trust them with my most personal information, they have an almost sacred duty to protect it."

Scott says consumers should take steps to protect themselves from cyber crime as well. "Pay attention to what websites you are browsing. Don't blindly click on email attachments, and don't open any screen-savers somebody sent you that may look cool. Use your common sense," says Scott.

The early reviews on Bullseye Breach have been very favorable. Ken Steinhardt, a computer scientist and retired former vice president at EMC Corporation says, "A Michael Crichton-like whirlwind story that is very hard to put down once you start. Part mystery, part suspense, part education, part technology, and all entertainment, *Bullseye Breach* is an extremely impressive first offering from author Greg Scott. You don't need to be particularly well-versed in IT to enjoy it, but you will be wiser after you read it."

Winn Schwartau, CEO of The Security Awareness Company, says, "A most ambitious look at the global security ramifications of the simplest error in judgement. How a single person, with little or no security awareness, triggers an escalating cascade of cyber-devastation on every continent. This is a perfect foray into how things can go terribly wrong... And all it took to get started was - One Thoughtless <Click>."

"Our whole country runs on the Internet today. If we don't take security seriously, the breaches we have seen so far will only be the beginning. You don't have to be a victim. It is not inevitable. Protect yourself," warns Scott.

Bullseye Breach: Anatomy of an Electronic Break-in is available for purchase at bookstores everywhere, as well as online at www.amazon.com and www.barnesandnoble.com. For more information, visit www.bullseyebreach.com.

About the Author

Greg Scott is a self-proclaimed computer nerd. He can trace his interest in computers back to 1971 when he was 13-years-old and in the 8th grade.

"I would sit down at the computer terminal, type in a program, then the computer would do what I told it to do. For a 13-year-old kid who thinks the way I do, that was the coolest thing in the world. I was hooked then and there," says Scott.

After high school, he attended Wabash College in Crawfordsville, Ind., where he spent much of his spare time working in the school computer lab. After graduation he secured a full-time position at an engineering school in Indiana, where he was in charge of the refrigerator sized administrative offices' computer system. A few year later, he started working at Digital Equipment Corporation in the Chicago area.

Scott was laid off in the early 1994 when Digital fell victim to a changing IT industry. His next move was to start up Scott Consulting, a company that worked directly with businesses to handle their computer networking needs. Scott sold that company in 1999, around the time the dot com bubble burst. Later that year, he started up Infrasupport Corporation with a laser focus on IT security and infrastructure.

After the Target data breach, and several other high-profile cyber crimes, Scott penned the novel, *Bullseye Breach: Anatomy of an Electronic Break-in,* with the intention of teaching people why it's so important for businesses—and consumers—to take steps to protect their electronic identities.

Learn more about Infrasupport Corp., at www.infrasupport.com. Information about Scott's debut novel, *Bullseye Breach: Anatomy of an Electronic Break-in,* can be found at www.bullseyebreach.com.

EDITOR'S NOTE: This feature article is being offered to you for use copyright free and cost-free. High resolution photography is also available for free upon request. If you prefer to work on your own story and want to schedule an interview with author Greg Scott, or request a review copy of *Bullseye Breach: Anatomy of an Electronic Break-in,* contact Rachel M. Anderson, Publicist, at 952-240-2513 or rachel@rmapublicity.com.

# # #

Title:	**Bulls**eye Breach
Author:	Greg Scott
ISBN:	978-1-5298-877-8
Book size:	6" x 9"
Pages:	240
Launch Date:	4/19/15
Copyright:	2015
Retail price	$18.95
Retail Price (eBook):	$9.98
Category:	Fiction
Publisher:	Beaver's Pond Press Edina, MN
Distributor:	Itasca Books www.itascabooks.com 1-800-901-3480 x118
Publicist:	Rachel M. Anderson RMA Publicity (952) 240-2513 rachel@rmapublicity.com