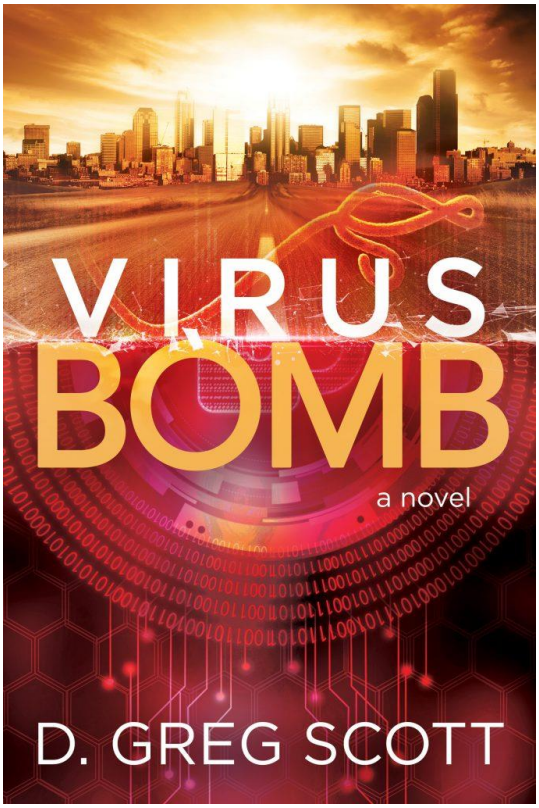
Can The United States Prevent A Deadly, Large-Scale Cyber-Attack?



What would happen if a nation-state really did launch a serious cyber-attack against the United States, perhaps as part of something larger?

Who will step up to save us – the government, big business, maybe a team of superheroes?

Or maybe a few ordinary people. Because real superheroes are ordinary people who step up when called. Even when they don't want to.

A new book explores what could happen when things go deadly wrong.

Minneapolis, MN -- D. Greg Scott, with 40 years of IT experience under his belt, including 15 years building firewalls and handling cybersecurity for dozens of organizations and thousands of people, delivers a fascinating look at what our nation could experience in the very near future – unless we take steps now to avoid a cyber disaster – with his newest novel, ***Virus Bomb*** (Morgan James, Trade Paper 240 pages, $17.95, ISBN:9781642791648).

So much can go wrong today – hacked files, financial theft, identity fraud, data breaches, ransomware. And then there is the big stuff.

In his book for nail-biting adrenaline junkies, author Scott dissects the technological details of an all-too-familiar cyberattack, and the all-too-familiar reaction from people who should know better. But this time, the country will pay dearly unless a few ordinary people step up. Scott hitches the imagination to a rocket as he launches the reader into the middle of a potentially devastating chain of events.

"*Virus Bomb* hits especially close to home because the real world is plagued with daily data breach headlines," asserts Scott. "And the public rarely learns the root cause behind these disasters. If we care about winning against the armies of attackers out there, we need to lift the fog around how these attacks unfold."

Scott is available to speak about the following:

- Why cyber-security threats are dead serious and we need to take them more seriously than our governments, businesses, and institutions do.
- Why those serving in the IT frontlines go under-appreciated as they struggle to keep us safe.
- How our smart devices and connectivity of everything may pose huge dangers to us.
- Why the government and big companies cannot stop the problem on their own, but rather it is individuals, like you and me, who need to educate and protect ourselves better.
- Why we need fiction to help us understand and improve the real world.
- Why Americans are fascinated by technology, fearful of terrorist attacks, and deeply concerned about their safety and data being compromised.
- How there are real superheroes amongst us, the ordinary who will step up to do the extraordinary.
- Trends he is seeing in cyber-security today.
- Why the 'good guys' need to collaborate and share information – just like 'bad guys' do.
- Advice for what needs to be done to improve our electronic grid of data and security – providing specific tactics and strategies to help us remain safe and secure online.
- What needs to be done to address major policy issues, including encryption, credit reporting industry reform, and net neutrality.

His book is authentic, based on not only real news accounts and his understanding of technology and cyber-warfare, but on first-hand research, which included listening to hours of cockpit recordings, interviewing law enforcement professionals, studying historical events, and learning about the practice of the Muslim faith. He combines his tech knowledge with a flair for action to deliver a roller-coaster ride.

Virus Bomb draws in a diverse audience of aviation enthusiasts, medical professionals, leaders in business and government, law enforcement officials, penetration testers, and everyday people. Using his decades of experience in the IT industry to flesh out the details in his book, Scott transports the reader to the brink of the largest cyber-attack in history, where the fate of thousands rests in the hands of "Jerry," the IT guy.

Will Jerry take matters into his own hands to protect his fellow citizens? Will Jerry be able to convince the bored and uninterested government officials of the importance of IT security? As Jerry's journey intersects with a young man who has been persuaded by foreign radicals, *Virus Bomb* provides a peek into the web of actors with ill-intentions.

More About The book

Jerry Barkley is a Minnesota IT contractor just trying to earn a living for his family. He's no superhero. He never worked for the government. He knows nothing about international espionage. And, so nobody believes his warnings when he uncovers the largest cyberattack in history. Somebody is gathering data to plan a series of bombings and a biological attack and trying to pin blame on a terrorist group. And the FBI thinks Jerry is part of it.

Hundreds are already dead. Thousands more could die, first from Ebola and then potentially from war with the wrong enemy. If he doesn't act, who will? Up against willful ignorance, a hostile law-enforcement bureaucracy, and armed with nothing but IT skills and quick wits, Jerry must leave his keyboard comfort zone and go face-to-face with elite foreign agents and shut this attack down.

Maybe Jerry Barkley is a superhero. Because real superheroes are ordinary people who step up when called.

Contact Information: Media Connect
Stephen Matteo 212-583-2776 stephen.matteo@finnpartners.ocm
Brian Feinblum 212-583-2718 brian.feinblum@finnpartners.com

D. Gregory Scott
Biography

D. Gregory Scott's career in IT spans four decades, including 15 years in cyber-security. For the last four years he has served as a senior technical account manager for Red Hat, Inc. providing a concierge service to support their most important customers.

He's the author of two books, ***Virus Bomb***, a thriller about what would happen if a foreign power really got serious about attacking the United States over the internet, and *Bullseye Breach: Anatomy of an Electric Break-In*, an IT security educational book disguised as a novel about how security failures at a fictional retailer allowed overseas attackers to steal millions of credit card numbers.

Scott, who spent twelve and a half years at Digital Equipment Corporation earlier in his career, has mastered extremely complex IT challenges in various roles as a vendor, end user, and published author, enabling customers to cut costs, increase security, improve efficiencies, and increase revenue.

Early in his career, he developed one of the very first computer-aided financial aid packages for college students. He also proposed, designed, and built one of the first on-line college data management systems in the world.

At Digital Equipment Corporation, he led development for one of the first and most reliable client/server applications ever built. He was the winner of the Digital Equipment Corporation VMS Partner Excellence Award, the Circle of Excellence Award, and the Software Services Excellence Award.

Scott also led the technical effort for Tailgating with the Troops in Wisconsin, connecting several hundred Wisconsin families with loved ones serving in Iraq. Although this effort has no financial metric, the benefit to United States military families is incalculable. He also built Linux firewall systems to manage family connections at several highly publicized events with the Minnesota Twins, Minnesota Vikings, and Minnesota Gophers, as well as St. Paul Chamber of Commerce, St. Paul Saints,
Tee It Up for Troops, and Serving Our Troops.

Scott has been featured in several media outlets, including WCCO-Radio, Northern Alliance Radio, KARE-TV, Fox 9 TV, *Twin Cities Business Journal, St. Paul Pioneer Press, Minneapolis Star Tribune*, and *The New York Times*. He has served as a columnist for both *ENT Magazine* and *Enterprise Linux Magazine*, writing about technology.

Scott taught entrepreneurship at Rasmussen College. He has a Bachelor of Arts from Wabash College, and an MBA in new ventures from University of St. Thomas. He holds several IT industry certifications, including CISSP number 358671.

He resides in a suburb of the Twin Cities in Minnesota. For more information, please consult: www.dgregscott.com.

D. Greg Scott
Q&A
Virus Bomb

1. **Greg, what inspired you to pen *Virus Bomb?*** While writing *Bullseye Breach*, I saw a small story on a back page in the St. Paul Pioneer Press about somebody who committed suicide after the Target data breach. That drove home for me that the stakes for cyberattacks are higher than just money. We're all interconnected these days and malicious online interactions really do contribute to people dying. And, so with *Virus Bomb*, I wanted to combine several elements. How and why does a teenager who grew up in the United States decide to join an overseas terrorist group? After the United States launched a software weapon against a hostile country, what happens when that country turns it back on us? At the grass roots, what happens when we purposely ignore the threats all around us because they come with technology words nobody understands? And in our interconnected world, how do ordinary people influence all this?

2. **How does it differ from your earlier book, *Bullseye Breach: Anatomy of an Electronic Break-In?*** *Virus Bomb* is a more aggressive story than *Bullseye Breach*. While *Bullseye Breach* shows how a fictional cyberattack unfolded, *Virus Bomb* focuses more on the consequences of a larger attack. I also applied lots of story lessons I learned from *Bullseye Breach* to *Virus Bomb*.

3. **Could the events in *Virus Bomb* really happen?** Yes. Many events in *Virus Bomb* have already happened in the real world.

   Consider the real-world cyberattack against the United States Office of Personnel Management (OPM) that made headlines in 2015. OPM allowed the Chinese to steal a roster and other information about every single US Government employee. OPM also allowed the Chinese to steal detailed information everyone who applied for a security clearance shared with the US Government. Imagine the spear phishing scams, blackmail, and other ways a hostile foreign power could exploit that information.

   Or consider the real-world 2008-2009 cyberattack the United States and Israel deny launching against the Iranians to slow Iran's nuclear ambitions. Iran has had 10 years to study that code and use it against us.

   Think about manipulating high government officials or other influential people into doing something stupid. In the real world during the 2016 election cycle, former Whitehouse Chief to Staff, John Podesta fell for a phishing attack and gave away his email password to the Russians, and the Democrats allowed the Russians to steal their private emails.

   Large-scale attacks are so common these days, they barely last one news cycle. Search for any Fortune 500 company name and "cyberattack" and the odds of finding a real-world attack story are better than even.

   Readers will find plenty of excitement in *Virus Bomb*. But no Hollywood hackers. Nobody needs

to suspend disbelief with this story.

4. **Is your book a warning to America that our present defenses against a deadly cyber-attack are woeful?** Yes, but it's more. A friend at Morgan James Publishing first presented these goals and I'm adopting them as my own. I also want to educate, inspire, and entertain people. And we need to pull our heads out the sand and take the kick me signs off our other sides.

5. **How did you go about researching the technical aspects of airplanes, law enforcement, the Muslim faith, and other central parts of your book?** I spent lots of late nights reading and listening to lots of material and talking to lots of people. Jerry Barkley spent a couple hours in the air, but it took me months to get him safely on the ground. I mentioned some of it in my acknowledgements; I had to find a good airport for him to land, I had to dig through Cessna documentation to figure out those instruments, and in airports, I buttonholed everyone I could find in a uniform when I was traveling for my job to try and figure out how the radio worked. I poured time and homework into every element of *Virus Bomb* because I wanted to get it right. I read lots of Muslim history around what Christians did during the Crusades and even while Columbus was discovering the new world. The backstories behind many of Jerry Barkley's interactions with the FBI are autobiographical. As are many of the cyber elements and characters. *Virus Bomb* is fiction, but I want it to be credible fiction.

6. **Tell us about the lead character, Jerry Barkley. Who is he?** He's a middle-aged, bald-headed white guy from Minnesota. He lives in a suburb with his wife of 30+ years, an adult daughter, and her two boys. He spent the first half of his career trying the climb the same corporate ladder as every other middle-aged suburban white guy. That didn't work out well, and now he's trying to get Barkly IT Services off the ground. He's been trying to get Barkley IT Services off the ground for more than twenty years. Some call him stubborn. He likes to think of it as persistent. He respects authority, but only to a point. He has a quick wit, a keen mind, and never enough money. But even if he had unlimited money, splurging for Jerry Barkley means buying a new washing machine instead of fixing the old one again.

7. **Your book is both entertaining and thrilling – as well as a bit of a warning and prescriptive text. Why are we fascinated with the big events that could destroy cities and kill millions?** I don't know – I'm just a bald guy from Minnesota. But when I look back to, say, the 1991 Gulf War, I spent money to bring cable TV into my house so I could watch live CNN coverage. I was busy at work during the 9/11 incident, but I spent every possible moment soaking up details and I still remember where I was and what I was doing. I also remember being glued to the news during the 2003 shock and awe campaign. I share the same fascination with big events, but I need to think more about why. It might be because I worry those events will turn my comfortable world upside-down.

8. **Your book seems to demonstrate how ordinary people step up and impact the world. How can we encourage others to see themselves as being potential heroes?** Real superheroes are ordinary people who step up, but many people want somebody else to step up. *Virus Bomb* has a character like that, and nothing and nobody will change her mind. How do we convince a skeptical business manager they're an unwitting global catalyst for catastrophe?

   In the real world, I used to play church-league, coed softball. I was never much of a softball player, and one time, a frustrated team coach tried to teach me about situational awareness. Know how many outs, where the baserunners are, the ball/strike count, and dozens of other factors. Always keep abreast of the game situation and how it affects me playing my position. This didn't help my hitting, catching, or throwing, but hopefully helped me make smarter game decisions.

This applies outside sports. They say when a bird lands on a power line in Canada, people in Mississippi feel it. In our interconnected world, somebody in North Korea can shut down a careless Fortune 500 movie studio with a few keystrokes. Or somebody in Ukraine can steal millions of credit card numbers from Minneapolis based Target Corp. by compromising an obsolete computer in an HVAC company in Pennsylvania.

We encourage others to see themselves as potential heroes by teaching global situational awareness. Start by reading *Virus Bomb* and *Bullseye Breach*.

9. **How can cyber-security be improved?** This is a multi-semester, graduate level college curriculum. But we can summarize everything busy people need to know about cybersecurity with a six-word rhyme. Care and share to be prepared. Care enough about your own security to learn and invest in what you need, share what you learn liberally, and expect all other good guys to share what they learn.

10. **You say that the bad guys are good at collaborating and sharing secrets on how to hack the Internet's vulnerable spots. Don't the good guys work together, too?** Not as well as we should. Look no further than the recent Capital One incident as a possible Exhibit A. Although we suspect somebody used a web application firewall as a weapon in a server-side request forgery attack, the specific exploit the attacker used to penetrate that network is still not public. Equifax offers another example. It took a Congressional investigation to produce a report on what went wrong. Don't believe me? Pick any Fortune 500 company at random, call the security department, and ask for details on how it protects itself. Good luck getting an answer.

11. **What should Americans do to protect their identity, key information, and online records?** Consumers can start by going to my website and signing up for Greg's cybersafety tips. Here's the URL:https://www.dgregscott.com/gregs-cybersafety-tips-landing-page/

    Organizations that sell goods and services over the internet should listen to my talk about adopting open. Here's a link: https://www.dgregscott.com/a-radical-not-so-new-idea-to-stop-the-daily-barrage-of-data-breaches/

12. **What do you suggest companies like Capital One or Equifax do to avoid another huge data breach?**
    a. Adopt open to reduce the probability of an attack. See above.
    b. Reform the credit reporting system to reduce the value of Social Security Numbers and therefore the value of any cyberattack. See my recorded presentation at https://www.dgregscott.com/143-million-reasons-credit-reporting-industry-reform-part-2/

13. **How can digital attacks on data get weaponized to the point terrorists can expose us to dangerous biological, chemical or traditional threats?** Back in 2008, the United States and Israel officially did not collaborate to sabotage the programmable logic controllers (PLCs) that controlled the Iranian centrifuges they used to refine Uranium. Somebody – the United States and Israel deny they were involved – sabotaged the software in those PLCs to spin the centrifuges faster than their rated capacity. This destroyed lots of centrifuges. Experts estimated this set the program back buy two years. All it takes is for software to open or close the wrong valve at the wrong time and somebody could blow up a nuclear power plant. Or worse. Or beyond direct targets, an attacker could penetrate, say, the transport industry, find details about shipments of dangerous materials, and go after those.

14. **What are some really dumb things you've seen in your many years in IT and cyber-security?** One of the dumbest was my own fault. Back in 1981, I was a rookie system admin for an engineering college in Terre Haute, Indiana, and I didn't pay close enough attention to running backups. After four weeks, I figured it was time. The backups got about 1/3 of the way through copying to tape before the heads crashed on the hard disk drive I was backing up. It was an uncomfortable meeting when I met with the director of the Registrar's department and told him I'd destroyed all his data. I never regained my credibility. Today, I tell people they aren't an IT professional until they've destroyed somebody's data and there's no recovery. Everyone should feel that feeling in the pit of their stomach once. And then remember it forever.

    Another time in the mid-80s, I was involved in a larger backup situation. This time, Delco-Reamy Electronics suffered a disk failure and had no backups. This one threatened to shut down all of General Motors around the world. It was right after GM bought EDS to operate its IT systems, and the original GM People thought EDS was running backups and EDS thought original GM people were doing it. They found out neither were doing it shortly after the disaster. Lots of corporate vice-presidents were on the phone with lots of other corporate vice-presidents about that one, and a few heroes lost lots of sleep over the next several days to piece it all back together. My only contribution to that one was attending lots of meetings.

    Maybe the best one was the time in Nov. 2000 when I had to explain to the FBI what the internet does. Here's a blog post with the ugly details: https://www.dgregscott.com/made-care-security/

    And speaking of the FBI – here's another one about the FBI and me. I'm sure the FBI has plenty of smart people, but I've seen plenty of government CYA from them over the years. https://www.dgregscott.com/the-fbi-and-bureaucracy-and-me/

    Oh – and the time I sat in front of a small bank vice-president and he showed me a copy of the security audit report the bank had paid a consulting company to produce. I looked through the report with lots of details on the probes they did against the bank website. When I asked what the consulting company found about the bank's internal network, the vice-president didn't know what I was talking about – he didn't know the difference between his bank's website and the computers his tellers used to accept deposits. He thanked me for coming and hustled me out the door.

    Another company put its server on top of a piece of plywood in a hot, dusty garage and never backed it up. It died one day and he lost everything. I met an accountant who wanted his company server in a hot furnace room. On a table right next to the furnace. And a bill collector in 2011 who still operated a Windows 2000 server. He hadn't backed it up in months and it failed the day I showed up to talk about it. I spent most of a day getting it back up and running. My reward – he yelled at me so loudly the walls vibrated.

    I had a charter school one time who wanted specs for a Windows Small Business server to handle 200+ users. When I told them Small Business Server had a limit of 75 users, they blew me off. I can probably come up with more after thinking about it.

15. **Do criminals and terrorists use the same tactics as nations do in the e-war battles fought online?** Yes. The only difference is, nations have more people doing more of it.

16. **We hear Russia, Russia, Russia. Are our elections compromised, not only by foreign propaganda, but by actual manipulation of electronic voting booths?** Not that we know of, although Kim Zetter – author of *Countdown to Zero Day* - and others have news reports of the

Russians trying to compromise voting machines. There's also good news here; DARPA is leading an effort to build an open source voting machine prototype for private companies to adapt for their own products. This is one of the few stories I've seen of enlightened government activity around cybersecurity.

17. **Over the past four decades in IT, with the last 20 years in cyber-security, what patterns have you seen emerge when it comes to a weak and compromised system of safety online?** Too many people are ignorant and proud of it. It's no different than reading literacy hundreds of years ago. Society today needs a new kind of basic literacy and we need to change attitudes.

18. **Should we trust Amazon, Google, Facebook and Microsoft to protect us?** About as much as we should trust Bernie Madoff with our investments.

19. **What trends do you see formulating in IT and cyber-security?** More consolidation into massive datacenters as everyone moves into the cloud. Tighter and tighter connectivity, with associated applications on top of that as we continue wiring the world with fiber. More sensational headlines about data breaches, more hysteria. But it will eventually improve as the technology and our attitudes mature, just like with earlier technology revolutions.

20. **Do we sometimes need fiction to present the truth to ourselves?** Yes. We've been using fiction to present truth for thousands of years.

21. **Why do so many companies and government agencies proclaim they'll do more to take cybersecurity threats seriously – and then huge data break-ins are discovered?** Too many business and political leaders consider IT as an expense instead of an asset. Until that attitude changes, the empty proclamations will continue. Many busy executives pay lip service to cybersecurity, but delegate it all to the IT Department with the mandate to do more with less. When Home Depot lost 56 million customer credit card numbers back in 2014, the Home Depot execs summed it up best when they said, "We sell hammers." Other busy execs get paranoid. They spend lots of money for security theater with checklist audits from third party companies, but never educate themselves on the fundamentals behind those audits. Proclamations are easy. Practicing due diligence, investing, and making informed decisions is hard work. So is leadership. And industry and government need leadership to tackle this problem. Somebody needs to lead the way into adopting open.

22. **Do we even really know how often our safety and data are compromised or threatened?** Sort-of. It's always threatened and already compromised.

23. **Why do you believe organizations should open up what they do for cyber-security and subject it to a gauntlet of peer review and public scrutiny**? Because bad guys spend all day probing good guys and all night collaborating to improve tomorrow's probes. But good guys isolate ourselves in the name of secrecy. That's why we keep making the same mistakes. The FAA investigates every plane crash and produces a post-mortem report for the whole world to see and argue over. Look for similar public reports about data breaches -they don't exist.

24. **Encryption. Cryptocurrencies. Smart homes. Driverless cars. Is the connectivity of everything exposing the world to a catastrophic danger?** More like new opportunities and new threats. Everyone liked cars better than horses and buggies even though car accidents are worse than horse accidents. Today, everyone likes their electronic devices better than paper and pencils.