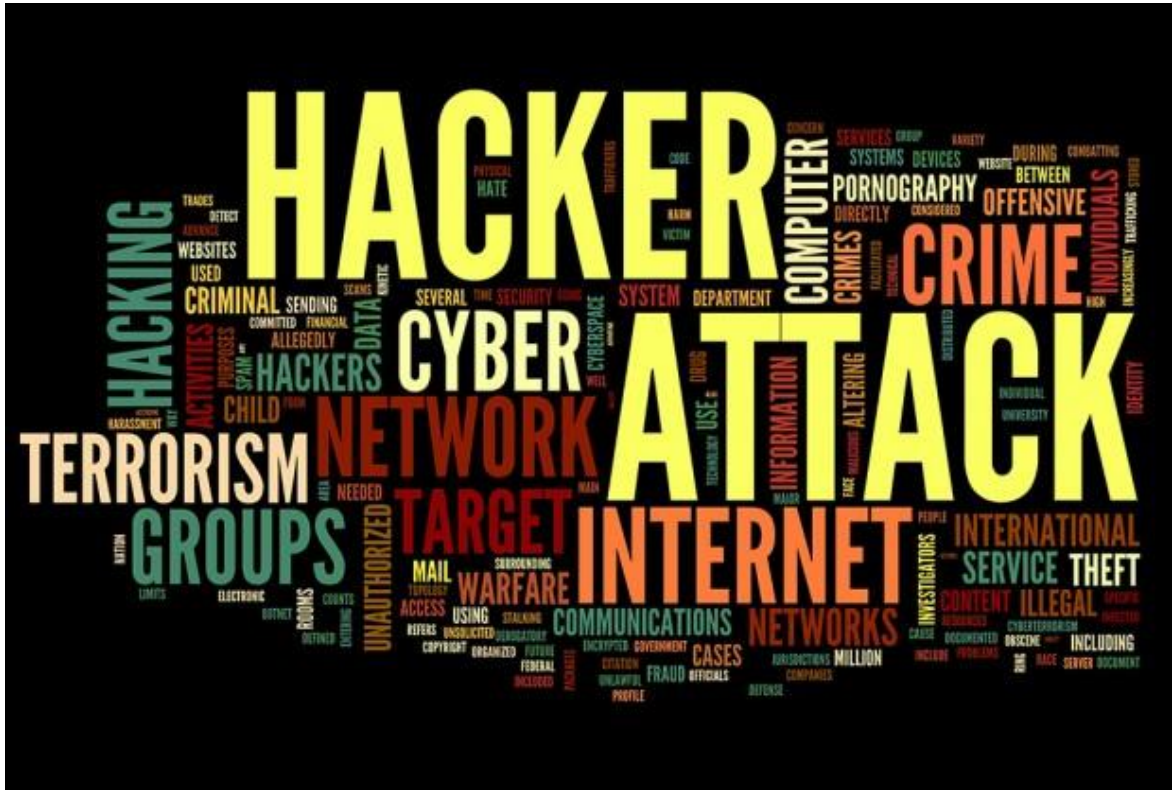
Morgan Lewis

YOU CAN'T MAKE THIS STUFF UP: THE FACT AND FICTION OF CYBERCRIME

Reece Hirsch, CIPP
Morgan Lewis & Bockius LLP

ISACA Fall Conference
November 9, 2015

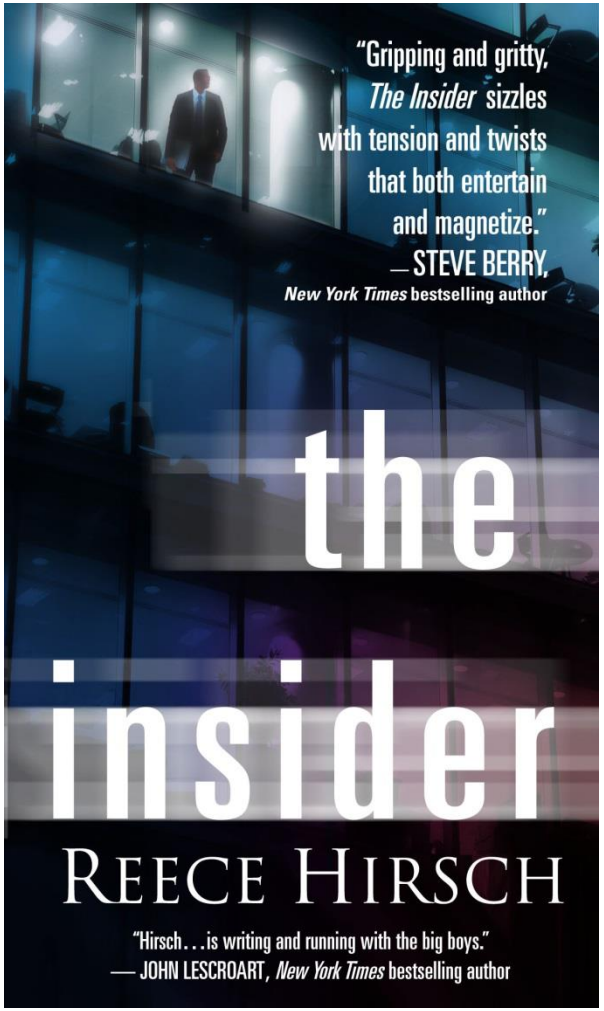
The High Drama of Cybersecurity



The Fact and Fiction of Cybercrime

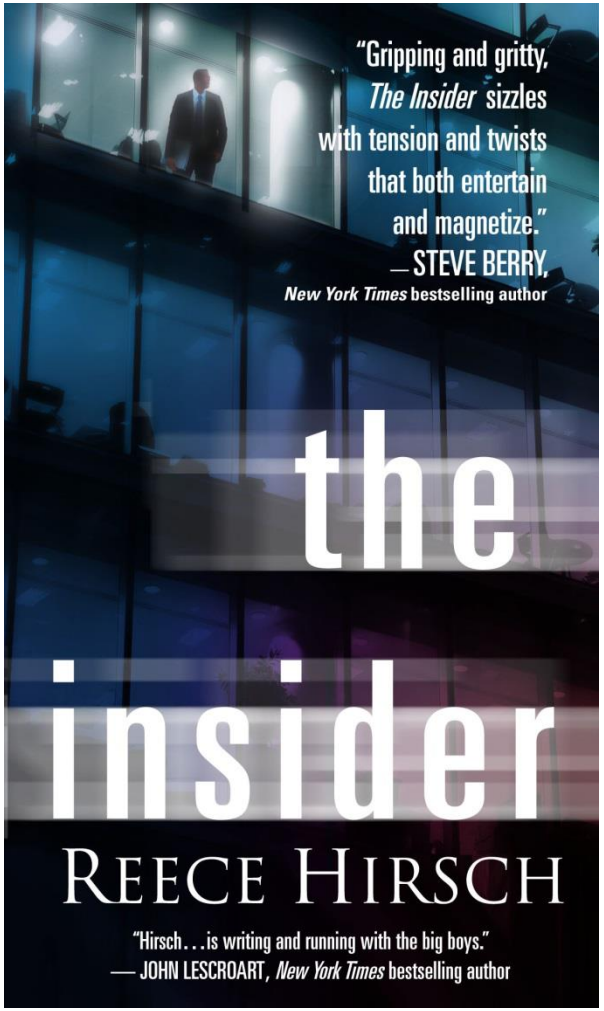
- The Book in the Drawer
- Started out inspired by Turow and Grisham, but soon began to draw inspiration from my privacy and cybersecurity practice
- Trying to stay at least a little bit ahead of the headlines
- Started as I was rewriting my first novel, THE INSIDER
- Will Connelly

The Clipper Chip



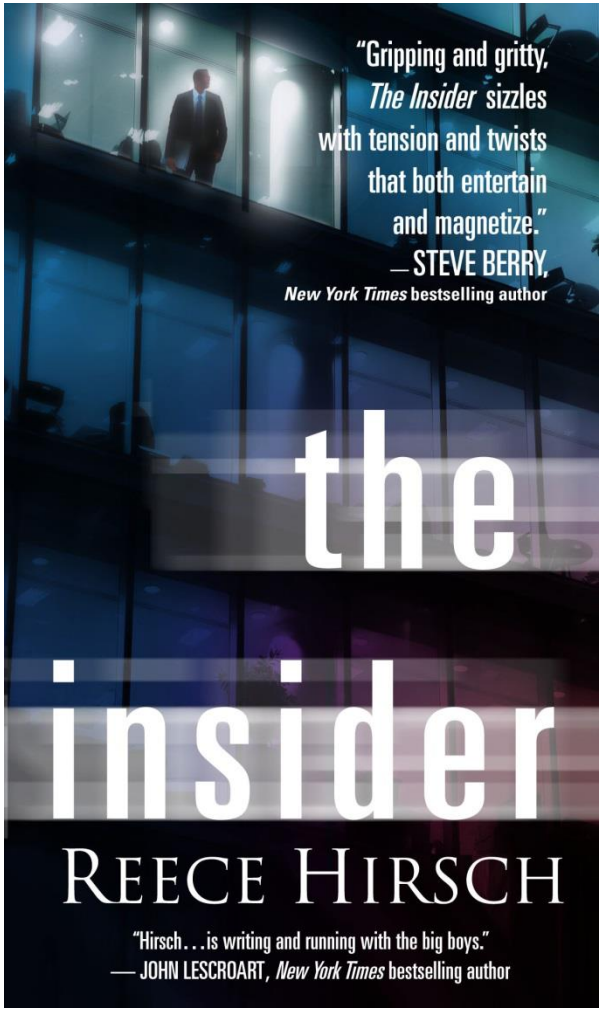
- In the early 1990s, the NSA developed a powerful encryption device known as the Clipper Chip
  - To be used to encrypt telecommunications transmissions
  - To be made available to private businesses and individuals
  - Clipper Chip was designed to provide "key access" to all encrypted transmissions for law enforcement and national security purposes

The Clipper Chip



- Program was criticized in Congressional hearings based upon privacy concerns and ultimately abandoned by 1996
- But what if the Clipper Chip program was never really abandoned?
- What if the program went forward through an undisclosed deal between the NSA and a private encryption software company?
- What if the NSA continued to secretly monitor the communications of private citizens during the ensuing years?

The Clipper Chip



- WHAT IF THE GOVERNMENT ENCRYPTION KEYS THAT PERMITTED GOVERNMENT ACCESS TO THOSE VAST VOLUMES OF PERSONAL INFORMATION FELL INTO THE WRONG HANDS?

Post 9-11 Government Surveillance

- December 16, 2005: the New York Times published a front-page story first revealing a covert, longstanding domestic surveillance program that had been conducted by the NSA under the Bush Administration in the years following the 9-11 attacks

- This was the other major inspiration for THE INSIDER – I imagined that such a program had been conducted since 1995, and had begun with the supposedly scrapped Clipper Chip program

- "The Watchers: The Rise of America's Surveillance State" by Shane Harris (2010)

Hepting v. AT&T

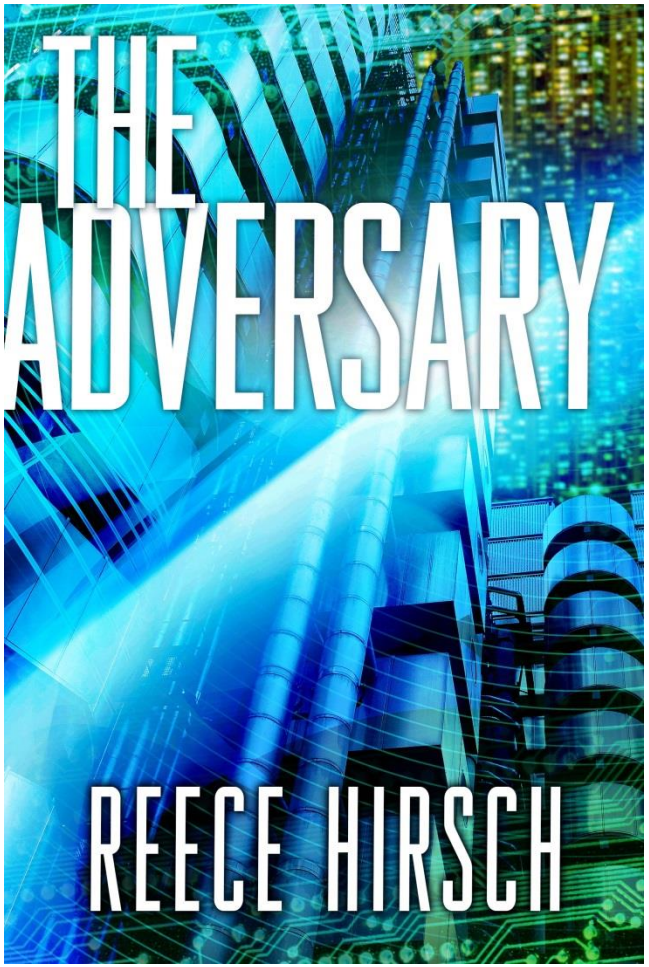
- January 2006: *Hepting v. AT&T*, a whistleblower lawsuit filed by the Electronic Frontier Foundation, alleged that specific AT&T facilities, including one on Folsom Street in San Francisco, had permitted the NSA to directly intercept and analyze millions of ordinary Americans' communications

- June 2009: a federal judge dismissed *Hepting* and dozens of other lawsuits against telecoms

- Government and telecoms were awarded retroactive immunity under FISA Amendments Act

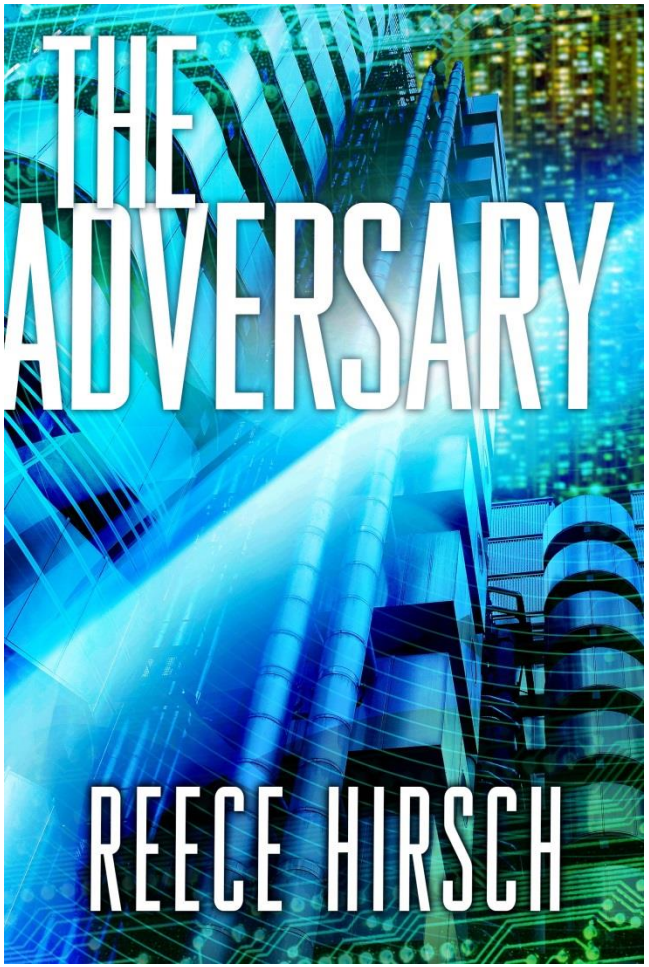
Stuxnet and the New Breed of Super Computer Viruses

THE ADVERSARY and Stuxnet



- 2010: Stuxnet was a computer worm or virus discovered in 2010 that was believed to have been created by the U.S. and Israeli intelligence agencies to attack Iran's nuclear facilities
- Stuxnet was designed to target only the centrifuges at Iran's Natanz nuclear enrichment center
- Causing machines to speed up or slow down and explode

THE ADVERSARY and Stuxnet



- Cyberweapons are not like bombs that are destroyed on detonation
- Stuxnet malfunctioned and failed to self-destruct
- Spread on the Internet (along with speculation about its source)

THE ADVERSARY Gets Real

- As THE ADVERSARY was being finished, David Sanger reported in the New York Times in June 2012
  - Stuxnet was part of a joint operation of the NSA and Israel's Unit 8200
  - Dubbed "Olympic Games"
  - Begun under President George W. Bush, expanded under President Obama
  - Reported to have set the Iranian nuclear program back by 18 months to 2 years

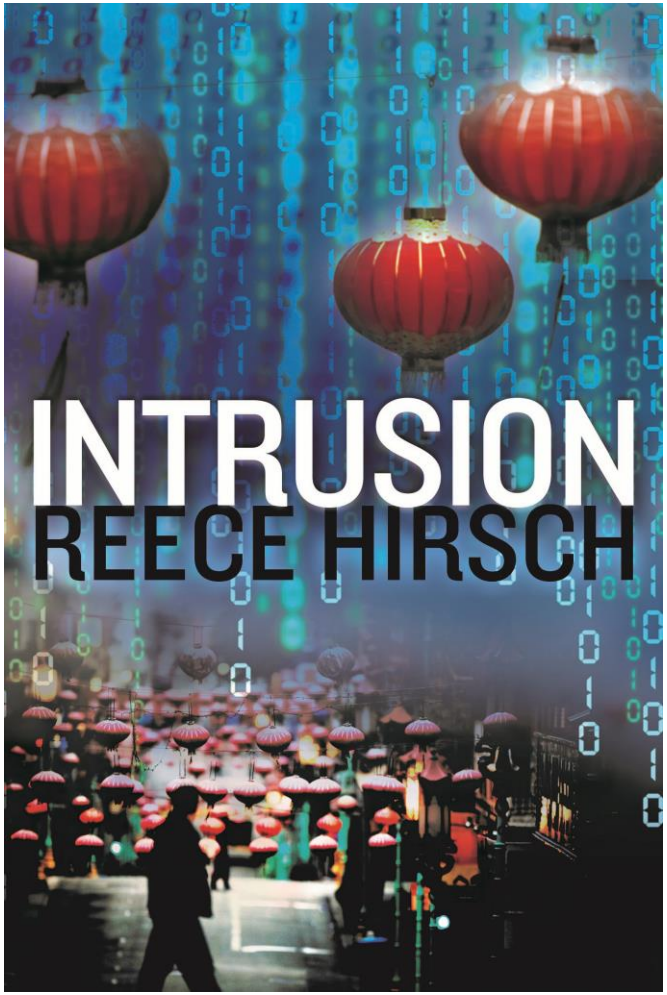
The Lurker Virus = Stuxnet

- The "Lurker Virus" in THE ADVERSARY is closely modeled on Stuxnet
  - Takes control of programmable logic controllers (PLCs), digital computers that govern a vast array of functions
    - From manufacturing assembly lines to the electrical grid
- New definitions of cyberwarfare
  - Warfare that can be conducted anonymously and by small groups of individuals
- Chris Bruen and Zoey Doucet

A "Cyber Hiroshima"

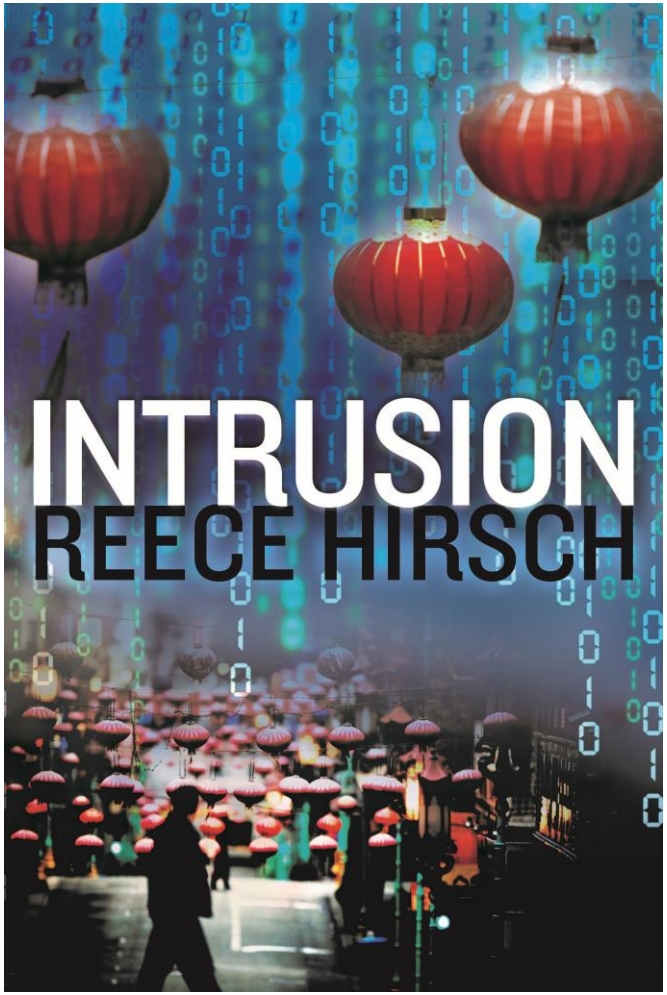
- Climax of THE ADVERSARY – a cyberattack on New York City
- Arrowhead Nuclear Reactor at Indian Point, NY near NY
- The dangers of a connected world, impact on supply chains
- A very real threat
- Fake call center ploy
- My Hurricane Sandy experience

INTRUSION and APT 1



- INTRUSION begins with Chris Bruen being called for a meeting in the middle of the night at the offices of the largest Internet search engine
- Based in part on 2011 hack of Google attributed to Chinese hackers
- Hiring top security talent and circling the wagons

INTRUSION and APT 1



- INTRUSION is also inspired by the Mandiant February 2013 report on APT 1, attributing it to China's People's Liberation Army
- Chris Bruen travels to Datong Road in Shanghai
- Chapter 3 of INTRUSION very closely mirrors Mandiant's real-life detective work

INTRUSION

- Assassins for hire on the Dark Net
- Big data analytics used to track a killer (courtesy of a search engine data analyst)
- Going inside an enormous riot that took place in one of the factories in Shenzhen, China that manufactures our laptops and smartphones

SURVEILLANCE – March 2016

- If THE INSIDER was my pre-Snowden NSA book, SURVEILLANCE is my post-Snowden book

- Ethical hacker operating a penetration testing firm learns about the existence of a secret government agency

- How will the NSA respond to the USA Freedom Act's limitations on bulk metadata collection?

SURVEILLANCE

- Inside the NSA's "Crypto City"
- James Bamford's "The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America"
- Laser microphones detecting sound waves on glass
- Quantum computing and the future of encryption

Dark Net/Silk Road Experts

- Bruce Schneier
- Looking for Dark Net/Silk Road experts for next book
- As long as there is personal information and people who want to steal it and spy on it, I will never run out of material

Questions?

Reece Hirsch
rhirsch@morganlewis.com
(415) 442-1422