Future Crimes
Marc Goodman

Why read this book?
“Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. And just over the horizon is a tidal wave of scientific progress that will leave our heads spinning—from implantable medical devices to drones and 3-D printers, all of which can be hacked, with disastrous consequences. With explosive insights based on a career in law enforcement and counterterrorism, leading authority on global security Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. He explores how bad actors are primed to hijack the technologies of tomorrow. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control of our own devices and harness technology’s tremendous power for the betterment of humanity—before it’s too late.” (Amazon)

Key Quotes
“And if data are the new oil, the modern currency of a digital world, then those in possession of the greatest amounts will have enormous power and influence.” (P. 106)

“Today, any company, large or small, can have a Snowden in its midst with notable implications for its data security, privacy, and long-term economic viability.” (P. 108)

“Real space will become just like cyberspace, and as all objects around us join the Internet of Things, any meaningful distinction between online and the off-line worlds will disappear.” (P. 295)

“As the use of drones and other robotic technologies becomes more commonplace, we can expect them to be leveraged by all members of society, for both good and ill.” (P. 370)

“Your goal is not perfect security; your goal is understanding how to lock the doors and windows to your car in cyberspace, and about that there is much you can control.” (P. 461)

“The future of cybercrime will be exponential, automated, and three-dimensional.” (P. 506)

“Machines are finally coming to life. After a long era of hibernation, they are ready to descend upon our physical world, and when they do, they will bring with them a tidal wave of threats for which we are wholly unprepared.” (P. 366)
Future Crimes

This is a book about

1. A Gathering Storm
2. The Future of Crime
3. Surviving Progress

A Gathering Storm (Part 1)

1. Mat Honan
   a. Lost I-Phone (remote wipe), Apple account, Google account, Twitter account.
   b. Billing address and last 4 digits of credit card
2. “The traditional transnational barriers to crime faced by former generations of thieves, thugs, and convicts have been demolished in the online world, allowing unsavory individuals to freely enter and exit any virtual location they please.” (P. 14)
3. We are living in a borderless world where jurisdiction is unknown, fingerprints and DNA immaterial.
4. Computer viruses, worms, Trojans, hackers, OH MY!
5. Security is an illusion: Threat detection success rates 5%, time to detect growing longer and hackers can successfully penetrate network defenses in minutes 75% of the time. (P. 21)
6. Jan 2008 a 14-year-old hacked into a city rail system in Poland and redirected trains in the city’s tram system derailing 4 trains.
7. “The electricity grid, gas pipelines, 911 dispatch systems, air traffic control, the stock market, our drinking water, streetlights, hospitals, and sanitation systems are all dependent on technology and the Internet to function.” (P. 26)
8. “Even Symantec, maker of pcAnywhere and Norton AntiVirus, has had it source code stolen. (P. 33)
9. “Traditional organized crime groups, such as the Italian Mafia, Japanese Yakuza, Chinese triads, and Colombian drug cartels, have all diverted efforts and resources from their usual criminal activities to take advantage of the easy profits, greater anonymity, and limited police scrutiny afforded in cyberspace.” (P. 33)
10. China’s hacking efforts have netted the nation the greatest transfer of wealth in human history.” (P.40)
11. Moore’s Law: predicted that the number of transistors per square inch on an integrated circuit would double every year into the future. Welcome to the exponential pace of change.
12. Social networks are the new public records. All that you share, wittingly or not, is being scraped, sorted, and warehoused by newly emerging global data behemoths and sold to advertisers, governments, and third-party data brokers, each with an increasingly voracious appetite to know the most intimate details of your life.” (P. 57)
13. Why are so many services that we previously paid hundreds of dollars for suddenly free? So that we can reveal an ever increasing volume of data about ourselves and our lives! You are no longer the customer – YOU ARE THEIR PRODUCT.

14. Terms & conditions – Facebook’s privacy policy more than twice as long as the U.S. Constitution (P. 71)

**A Surveillance economy**

1. Could what you post online be used to charge you with a crime in the future? Picture of 20-year-old drinking wine at the dinner table; taxes not paid; who you have phoned; where have you been...
2. They know more about you than you do! Father learned of his daughter’s pregnancy because Target had a prediction algorithm from data purchased from data brokers. (P. 91)
3. Your posts are fair game to attorneys as evidence
4. Social media and cell phones are the great surveillance programs of the CIA and FBI
5. They know where you are (or aren’t). Posting blogs of your trip? Well you aren’t home!
6. But if you don’t own your Social Media, someone else might create it for criminal activity.
7. 90% of all mobile malware is targeted against Google’s Android mobile operating system.
8. And if you jailbreak your IOS model it then opens the device to the same security threats Android users face.
9. Snapchat photos DO NOT self-destruct and can still be retrieved.
10. 89% of employees are accessing work-related information on their mobile phones, and 41% are doing so without permission of their companies. (P. 139)
11. Tracking your location increasingly easy to do. Is a badge on Foursquare or a check-in worth your life?
12. There is no such thing as “standard Google”. What you see, watch or consume online is tailored for YOU. More and more of what we “SEE” is filtered.
13. And what we see may not even be what it is – crime ware exists that can change what you see – bank statements, credit card transactions... in real time (P. 174)

**The Future of Crime (Part 2)**

1. Organized crime is believed to account for up to 15 to 20 percent of global GDP.
2. Criminal gangs at airports use information on chauffeurs’ signs to Google the executives on their smart phones and determine their corporate positions and net worth. Several executives were kidnapped and others killed. (P. 223)
3. Read the story of Dread Pirate Roberts, the mastermind behind Silk Road, a massive online criminal marketplace. Who was this mastermind? Ross Ulbricht, Eagle scout with a master’s degree in engineering, from Austin, Texas.
4. Enter the matrix: the Deep Web or Dark Net or Secret Web or Invisible Internet.
6. Cars often have a small black box (some used by dealers for repossessions). An intruder illegally accessed a website and began turning off cars throughout the city of Cleveland. There are millions of cars around the world that can be controlled one way or another online.
7.  2013 – 13 billion online devices; 2020 – estimate is 50 billion things connected to the Internet (NOTE: Kiplinger has those numbers at 6 billion and 20 billion)

8.  Internet of Things (IoT) means that all physical objects in the future will be assigned an IP address & transformed into information technologies, making it possible to remotely control any object on earth.

9.  School officials across the United States have begun embedding RFID chips in student identity cards, which pupils are required to wear on their persons at all times. (Andrea Hernandez in San Antonio was suspended when she refused to wear her RFID device on campus.) (P. 297)

10. The Defense Department has already deployed a 1.8 – gigapixel camera that can be attached to a drone and spot targets “as small as six inches at an altitude of 20,000 feet”. (P. 305)

11. Since 2002 nearly all photocopiers have come with internal hard drives that store every document copied or scanned. (hackers have been able to access networked copiers and watch what was being copied in real time).

12.  We are all Cyborgs now – our phones are external brains and additional means of communication.

13.  Malfunctioning medical devices are one of the leading causes of serious injury and death in the U. S.

14.  Coursera use keystroke recognition to ensure the same student “attends” each virtual class.

15.  Robots
   a.  RiSE – a six-legged robo-cockroach
   b.  Cheetah – runs at nearly 30 miles per hour
   c.  BEAR – can lift and carry an injured soldier off the battlefield
   d.  Telepresence robots – allows people to move virtually through a distant building
   e.  Roomba
   f.  Drones
   g.  First case of robotic homicide was in 1981 – Kawasaki Heavy Industries
   h.  Robotic bumblebees and dragonflies

16.  3D printers can print human tissues, organs, ibuprofen, firearms and can self-replicate 50% of its own parts. By 2018 3D printing will result in over $100 billion in intellectual property loss globally.

17.  Artificial Intelligence is projected to reach human levels by around 2029.

18.  Biotech, Nano technology, quantum physics and space technology are next-gen security threats.

Surviving Progress (Part 3)
*The problem is not that technology is bad but that so few understand it.*

1.  Software developers need to understand and be held to higher standards to write more secure code.
2.  Develop a more consumer-friendly data protection directive like EU approach and limit what data companies can store and how long they can keep it.
3.  Kill the password and move towards biometrics combined with multifactor authentication.
4.  Use encryption by default
5.  Set a goal for citizens to have a basic understanding of how the technologies around them operate. Education for both the private sector and businesses.
6.  Adjust our own human behavior to significantly improve our personal technological security. “Lock our cars and turn on the alarm”.
7.  Human-centered product design is fundamental to drive the behavioral changes we require in the world of techno-security and to help minimize the growing number of threats we face.
8. Our goal should be to create a variety of sensors across our global networks to not only detect intruders and how they gained entry but, more important, automatically make the necessary repairs – a self-healing network.

9. Criminal laws, sovereignty issues, international law, criminal investigations, enforcement resources need to step up their game. (see page 467)

10. Practice safe Tech: the need for good cyber hygiene
   a. Application white listing
   b. Patch all your devices
   c. Patch operating systems by automatically updating
   d. Restrict admin privileges and only log in as admin when you need to

11. A trusted international cyber World Health Organization could foster cooperation and collaboration across companies, countries, and government agencies.

12. An XPRIZE for cyber security could serve as an engine of innovation.

---

**Headlines from THE KIPLINGER LETTER dated Dec 9, 2016**

- As sales of web-connected things take off...criminals have millions of new targets
- A major gnawing fear: A catastrophic attack
- Business disruptions will be unavoidable
- The cost to firms will run into the millions
- Manufacturers of devices susceptible to hackers face few consequences
- Moreover, many products are designed by firms with no security expertise

---

**UPDATE Protocol**

1. Update frequently – especially browsers, plug-ins, media players and Adobe Acrobat
2. Passwords – long (20 characters or more with upper/lower case letters, symbols and spaces). Use wallets such as LastPass, KeePass, Dashlane or IPassword. Use two-factor authentication
3. Download only from official sites and be very cautious of free software. Whitelist and pay attention to permissions e.g. access location or contacts
4. Administrator – use account with care. Log on as a general user whenever possible
5. Turn Off – turn off your computer when you are not using it. Same is true of your smartphone
6. Encrypt your digital life (bitlocker and fileVault) and use VPNs vs. public Wi-Fi networks

**Additional tips**

1. Use common sense with all your e-mail. Don’t open attachments without care
2. USB drives are dangerous. Disable “auto run”
3. Back up your data frequently. Carbonite, BackBlaze, SpiderOak, time machine
4. Cover up your camera
5. Sensitive browsing should be done only on your computer or a trusted computer on a trusted network
6. Think before you share on social networks
7. Use built in firewalls.
# Our Faculty

<table>
<thead>
<tr>
<th>Peter Braeuler</th>
<th>Mark Wittig</th>
<th>Malcolm Coon</th>
<th>Robert Schmidt</th>
<th>Judy Zimmerman</th>
<th>Andrew Wittig</th>
</tr>
</thead>
</table>

---

## 2017 Calendar

<table>
<thead>
<tr>
<th>Event Title</th>
<th>UTSA EMBA Alumni</th>
<th>Houston – Wittigs 11:30 – 1:00</th>
<th>San Antonio – Wittigs 8:00 – 9:30 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future Crimes</td>
<td>Jan 6</td>
<td>Jan 26</td>
<td>Jan 27</td>
</tr>
<tr>
<td>Then Inevitable: 12 tech forces shape future</td>
<td>Feb 3</td>
<td>Feb 23</td>
<td>Feb 24</td>
</tr>
<tr>
<td>Hunting in a Farmers World</td>
<td>Mar 3</td>
<td>Mar 23</td>
<td>Mar 24</td>
</tr>
<tr>
<td>Grit: The power of passion and perseverance</td>
<td>Apr 7</td>
<td>Apr 27</td>
<td>Apr 21</td>
</tr>
<tr>
<td>EntreLeadership</td>
<td>May 5</td>
<td>May 25</td>
<td>May 26</td>
</tr>
<tr>
<td>Secrets of the Millionaire Mind</td>
<td>Jun 2</td>
<td>Jun 22</td>
<td>Jun 23</td>
</tr>
<tr>
<td>Procrastinate on Purpose</td>
<td>Jul 7</td>
<td>Jul 27</td>
<td>Jul 28</td>
</tr>
<tr>
<td>Daring Greatly</td>
<td>Aug 4</td>
<td>Aug 24</td>
<td>Aug 25</td>
</tr>
<tr>
<td>Better than Before: What I learned about my bad habits</td>
<td>Sep 8</td>
<td>Sep 21</td>
<td>Sep 22</td>
</tr>
<tr>
<td>Ego is the Enemy</td>
<td>Oct 6</td>
<td>Oct 26</td>
<td>Oct 27</td>
</tr>
<tr>
<td>Leaders Eat Last</td>
<td>Nov 3</td>
<td>Nov 16</td>
<td>Nov 17</td>
</tr>
<tr>
<td>Winning</td>
<td>Dec 1</td>
<td>Dec 14</td>
<td>Dec 15</td>
</tr>
</tbody>
</table>

---

## Books

- Future Crimes by Marc Goodman
- The Inevitable: How Driverless, Urban Airports, and the Healthcare Robot Will Change Everything by Kevin Kelly
- Hunting in a Farmers World by Marc Goodman
- Grit: The Power of Passion and Perseverance by Angela Duckworth
- EntreLeadership by Angela Duckworth
- Secrets of the Millionaire Mind by T. Harv Eker
- Better than Before: What I learned about my bad habits by Ryan Holiday
- Ego is the Enemy by Simon Sinek
- Leaders Eat Last by Jack Welch
- Winning by Jack Welch