Cyberattacks Can Bring Down Factories and Stop Hearts. So Now What?

Cyberattacks are most often associated with data breaches or data theft. It's a big deal to us when our credit card information is stolen, our social security numbers are ripped off and someone pretends to be us as they tool around the country in a rented convertible on our tab. You're welcome.

But the bad guys can do more than shop. They can cause actual physical harm to property, businesses and human beings by hacking their way into machinery, appliances, toys, drones and medical devices.

On Dec. 1, 2016, the BBC® reported findings by researchers at the University of Leuven in Belgium and the University of Birmingham in England of "fatal" flaws in the radio-based communications systems of 10 different types of medical implants, including pacemakers.

"The consequences of these attacks can be fatal for patients as these messages can contain commands to deliver a shock or to disable a therapy," the researchers warned. One of them, decidedly understated cardiologist Rik Willems of Leuven, told BBC that "security must urgently improve." *(Fatal Flaws Found in Medical Implant Software, BBC, Dec. 1, 2016.)*

This stuff actually happens, and has been happening more and more this millennium. Because so much is run remotely over the internet, things we don't even think about anymore, the threat is real.

Surely this is a "glass half empty" situation, right? It can't all be gloom and doom. Actually, it's pretty gloomy and doomy. For more frightening details, last year Lucy L. Thomson of Livingston PLLC in Washington, D.C., wrote an excellent piece outlining them for the ABA Litigation Section, Insurance Coverage Litigation Committee. Thomson chronicles a number of ways hackers have managed to derail trains and shut down vital hospital HVAC systems and much more.

And these guys are no rays of sunshine either. David Navetta of Norton Rose Fulbright, Oliver Brew of Aspen Insurance and others on a panel at the *NetDiligence Cyber Risk & Privacy Liability Forum,* flashed these headlines on the big conference screen:

- *Fiery Pipeline Blast in Turkey Could Rewrite History of Cyber War*
- *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*
- *Hack Attack Causes 'Massive Damage' at German Steel* Works

These headlines don't even need exclamation points. "Although actual recorded cases of physical damage caused by cyberattacks are limited so far, their potential is vast," Brew told the *LexisNexis® Corporate Law Advisory*. "In many cases, the 'Internet of things' and connected devices have not been designed with security in mind.

"This makes the potential for exploiting these for access and denial of service attacks very significant," Brew said. "The recent DYN domain name server attack is a case in point," he said. "CCTV cameras were exploited to launch a massive denial of service attack, which caused outages at some of the largest websites, particularly in the Northeast U.S."

Privacy by Design

"Now that it is affordable to do so, we can find processors and software in common, household devices," Ronald I. Raether, a partner with Troutman Sanders LLP, told the *LexisNexis Corporate Law Advisory*. "The benefits are enumerable. To avoid the inconvenience of having to return to the grocery store because you forgot milk because your refrigerator has a running inventory can be invaluable.

"However," Raether continued, "with processing power and connectivity, these devices become a natural target for hackers. We see in the 'Internet of things' a pattern that has been repeated when technology has made its way into other devices or industry verticals. The initial focus is on providing the consumers the required functionality in the most efficient way. Privacy and information security issues may not be anticipated. The issue remains the same—finding the proper balance between allowing the devices to provide the conveniences desired by consumers while including the technical

and administrative controls needed to avoid any misuse of the systems. Thus, business operations which before have not had to address these technical issues must now become familiar with concepts such as 'Privacy by Design' and 'Defense in Depth.' As we have seen in prior iterations, it is a matter of education and consideration."

Another development that makes life even harder for security good guys is the so-called "industrialization of attack-ware."

Hacking for Dummies

"Online hacking tools have become commonplace, even with wizard-based applications allowing an unsophisticated hacker with malicious intent to cause havoc," Aspen's Brew told the *LexisNexis Corporate Law Advisory*. "The good news is that regulators are increasing their focus on this area, with new frameworks being introduced in order to drive improvements in security infrastructure. This is driving increased investments and awareness among key industries."

These risks are of critical importance to risk managers across the board, but some industries are more vulnerable than others, according to Navetta and Brew. They are oil and gas, manufacturing, pharmaceutical and agriculture.

Executive Order

"Concern for these critical infrastructure issues received additional attention," they said, "with President Obama's February 2013 Executive Order 13636, titled 'Improving Critical Infrastructure Cybersecurity'."

Citing repeated cyber intrusions into critical infrastructure, the president called it "one of the most serious national security challenges" facing the nation today. EO 13636 encourages shoring up the security and resilience of critical infrastructure. It calls for a cyber environment that "encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Attorneys John Buchanan and Dustin Cho of Covington & Burling recently wrote that not all of these events hit the front page. "In addition to the many common consumer products and medical devices that can be reached via the internet, military and consumer drones are also vulnerable," they said.

(See Buchanan and Cho's article—*When Things Get Hacked: Coverage for Cyber-Physical Risks*—written for the ABA Litigation Section, Insurance Coverage Litigation Committee conference held in Tucson, AZ, March 3, 2016.)

Insurance Covers What Now?

"The problem with most of the currently available cyber insurance products is this: They expressly exclude physical bodily injury and property damage," Buchanan and Cho wrote. While this may have been to avoid duplicating coverage offered by traditional policies, the question is this: Do they cover physical perils, like a train going off the rails?

Comprehensive General Liability (CGL) policies have been revised over the years in light of cyber risks. Variations have either said nothing, or that data are not property, or they included a "limited bodily injury exception." Or the policies specifically excluded coverage for damage arising out of data losses regardless of whether the damages are because of injury or damage, defined as any access to confidential, personal, proprietary or "nonpublic information," something that was not defined.

Buchanan and Cho—who represent major policyholder companies—interpret exclusion from coverage of "nonpublic information" *not* to exclude "all traditional bodily injury and physical damage caused by hacking of industrial control systems, malicious or negligent alteration of medical device settings, or other types of access to nonpublic electronic data that regulates networked 'things.'"

Again, forms vary on whether they expressly carve out bodily injury. But they also contain exclusionary language that bars coverage for loss of data, something that does not necessarily occur in a cyberattack.

Buchanan and Cho said an "aggressive insurer" might, however, argue that a hacker, by overwriting instructions in a device to enable him to do what he wants, could constitute damage or corruption of data, which they would argue is excluded. But, Buchanan and Cho write, such physical harm does not

"arise out of" the loss of original data, and cannot be "damage to" or "corruption of" data. "Harm arising out of such new data does not arise out of 'damage to' or 'corruption of' the old data within the meaning of this exclusion," they said.

Buchanan and Cho offer this advice to companies:

- Understand the potential cyber-physical risks you face.
- Analyze all of your current lines of coverage to determine whether and how each would respond to those risks.
- Seek clarifications in your current insurance wordings.
- Explore new "difference in conditions" insurance products designed to plug any gaps in coverage for such risks.
- Expect disputes with your insurers should these novel cyber-physical harms materialize.

Physical Perils Aren't Going Away

"In a world that is increasingly connected and automated, physical perils are serious risks that cannot be ignored," Mark C. Mao, a partner with Troutman Sanders LLP, told the *LexisNexis Corporate Law Advisory*.

"When hackers attack connected cars or life-supporting devices running on artificial intelligence, they create physical dangers to not only the individual users but everyone around them," Mao said. "It is critical that organizations continue focusing on securing communication networks and power grids, in addition to using only trustworthy vendors and suppliers. Physical perils will only increase without increased attention to how the world becomes more vulnerable as it becomes more connected and automated."

This article was edited for LexisNexis by Tom Hagy, managing director of HB Litigation Conferences and former publisher of Mealey's® Litigation Reports.