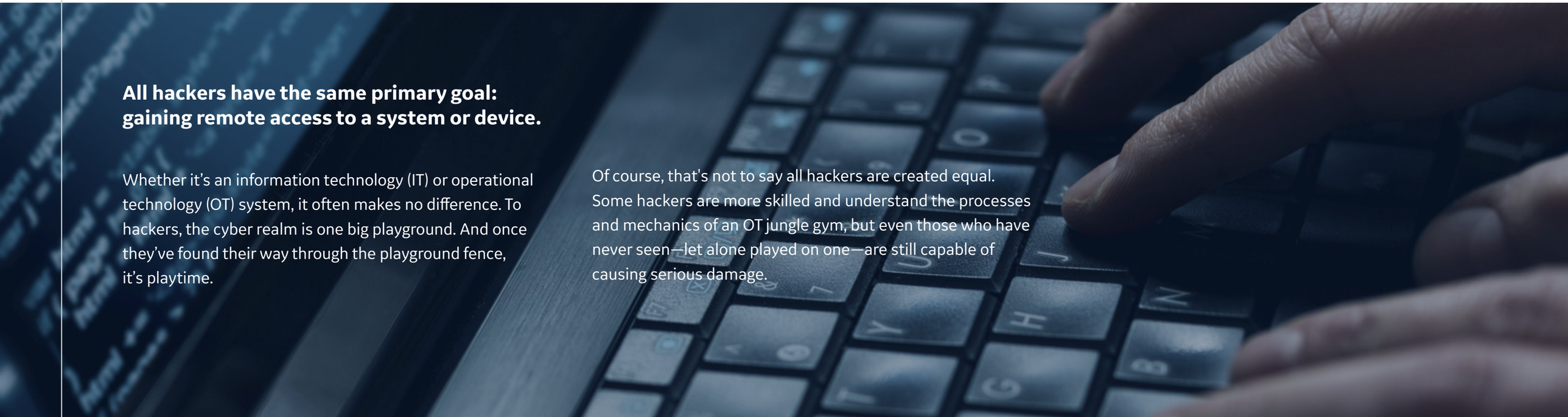
Cyber Attacks: It’s One Big Playground



All hackers have the same primary goal: gaining remote access to a system or device.

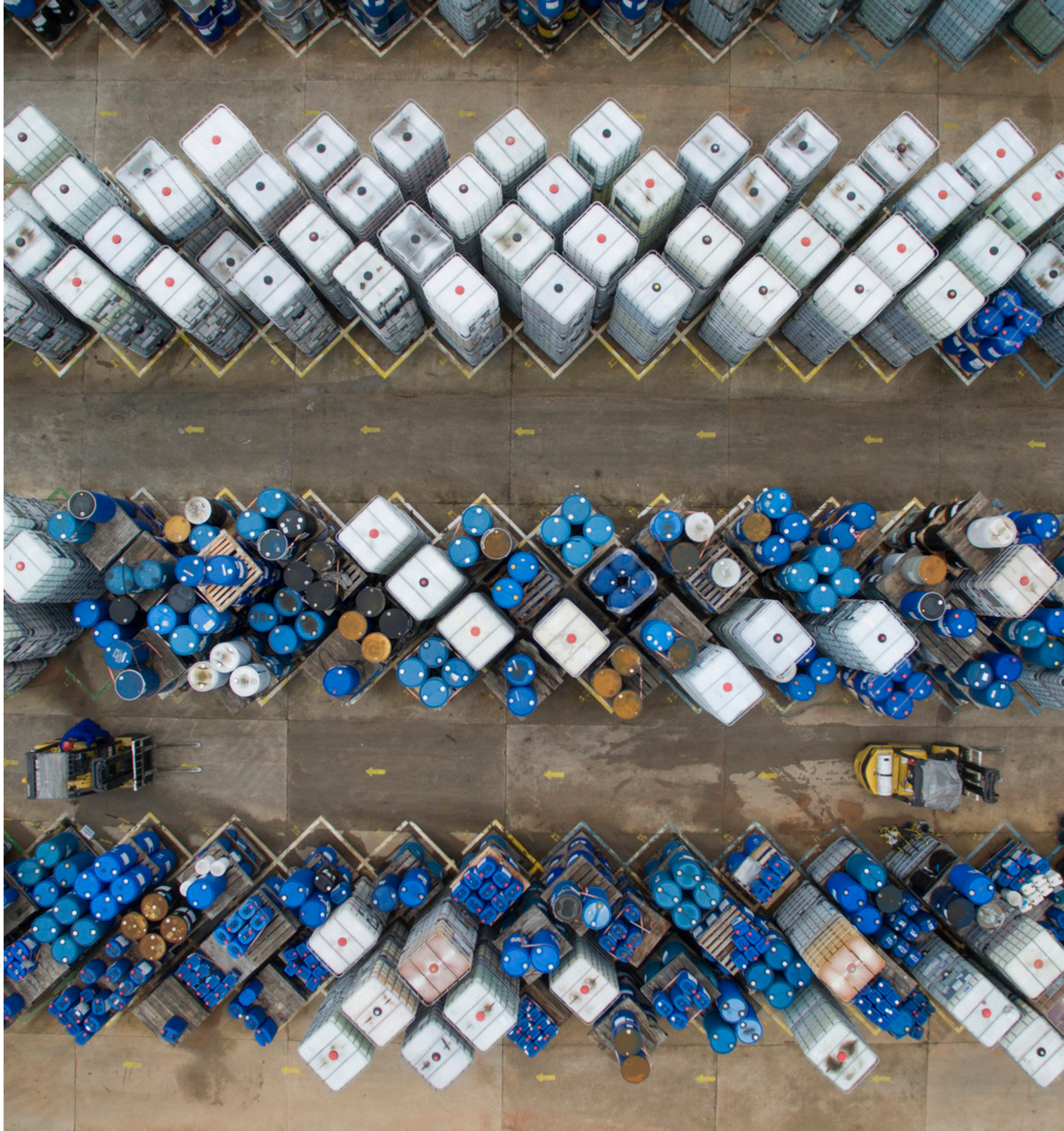
Whether it’s an information technology (IT) or operational technology (OT) system, it often makes no difference. To hackers, the cyber realm is one big playground. And once they’ve found their way through the playground fence, it’s playtime.

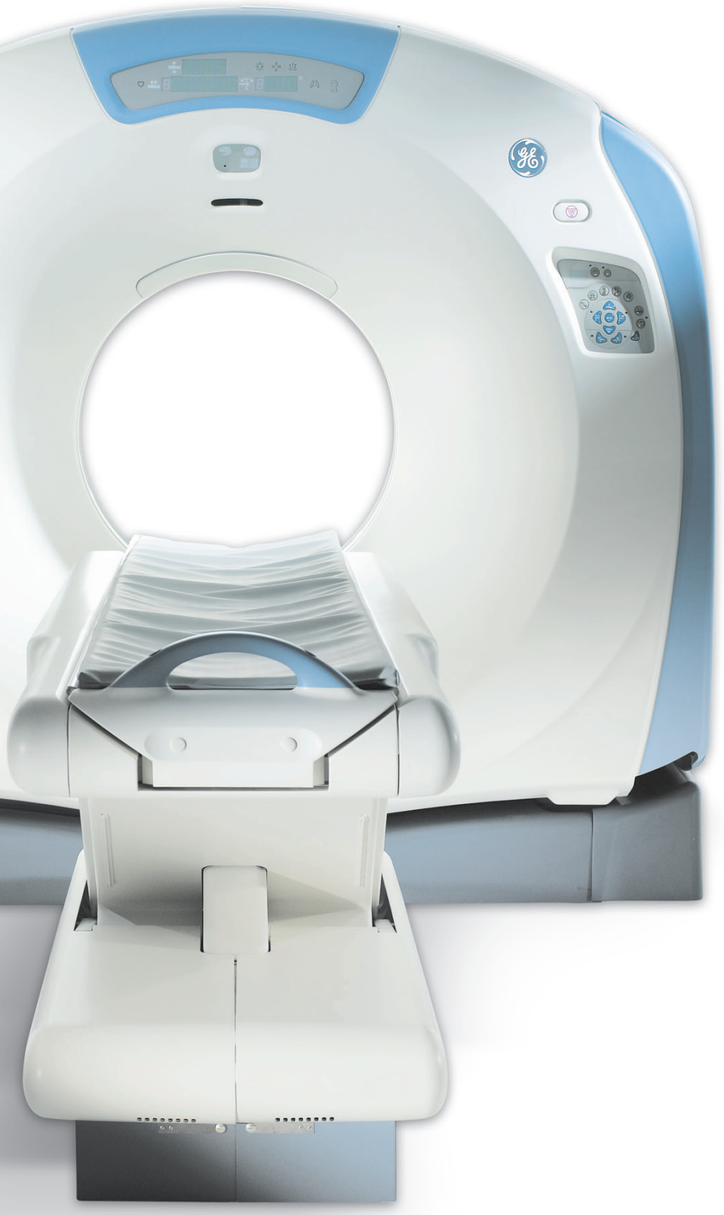
Of course, that's not to say all hackers are created equal. Some hackers are more skilled and understand the processes and mechanics of an OT jungle gym, but even those who have never seen—let alone played on one—are still capable of causing serious damage.

One thing leads to another

Enterprise systems, which are about data (e.g., email, Web, enterprise resource planning, financial management), are being increasingly connected to operational systems, which are about process (e.g., producing power, pumping oil, making chemicals). Even a relatively low-skilled cyber attacker can buy hacking tools to probe an enterprise system and potentially gain access into that system. If that system is connected to others and not properly protected, that intruder may have the ability to move from a Web server to an enterprise resource planning (ERP) system to a network gateway, and, in a worst-case scenario, all the way to a critical OT resource—such as a controller running a catalytic cracker in an oil refinery. It may seem like a big leap, but it's feasible when all of those systems co-exist within a company's enterprise systems.

Once on the enterprise system's "playground," a hacker may have the ability to explore such systems in greater depth, going from connected device to connected device, or from network layer to network layer, just as a burglar might walk from room to room in someone's house. When an organization doesn't have adequate visibility or security enforcement programs in place, hackers of any genre can spend weeks, or even months undetected, poking around a network until they filter out data for exploitation and monetization or, worse, maliciously disrupt a system.





In a way, the problem is not so different from what occurred with the infamous Sony breach, where "hacktivists" gained remote access to the company's network, stole and wiped private data, and advertised their victory via a skeleton screensaver across the company's corporate systems. In the end, final consequences included loss of information, loss of face, and loss of monies.

Had the same type of memory wipe happened in an OT environment without safety systems to protect against physical failures, the result could have been an unplanned, catastrophic, and dangerous shutdown.

The value of trade secrets

The more criminally minded, looking to exfiltrate and monetize information, might attempt to extract "secrets." IT secrets include things like credit card numbers, user names, and passwords. On the OT side, secrets might include things like electronic medical records (EMRs). While a credit card credential can sell for tens of dollars on the black market, a medical record can bring in hundreds to thousands of dollars. Why? Life expectancy. The ability to detect falsified medical records and billing claims is so difficult that an EMR maintains its value for much longer than a credit card.

The medical field is ripe with opportunity for hackers. Consider a hospital's diagnostic imaging systems. If attackers can gain access to magnetic resonance imaging (MRI) or computed tomography (CT) systems—which are part of a hospital's operations—they could alter records or treatment plans. What about data exfiltration in the pharmaceutical industry? Closely guarded trade secrets might include the recipes of chemical compositions or production processes and costs. Hackers understand and bank on how that type of insight could be incredibly valuable to a competitor, especially one who wants to substantially reduce research and development costs. These are just a few examples of how hackers can wreak havoc on your business's confidential information.

But what about another way—like ransomware? According to Cyber Threat Alliance, CryptoLocker ransomware generated $325 million for hackers within 100 days of its launch[1]. At the Black Hat 2016 CISO Summit, several industry experts projected a billion dollars would be paid in ransomware in 2016. In June of 2016, for example, the University of Calgary paid $20,000 to hackers to restore their information[2].

Now, just imagine that you are running an oil refinery and ransomware pops up on your operations consoles. Think about the cyber-physical consequences of disruption. You've got this big, dangerous process running, and all of a sudden somebody takes away your access to the control system. Now you can't speed it up, you can't shut it down, you can't do anything. That's no longer just a confidentiality or financial problem. That's a serious situation that puts profits, processes, assets, and lives in jeopardy[2].

1 *"Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat," Cyber Threat Alliance, (September 2016).*

2 *BBC News, "University pays $20,000 to ransomware hackers", June 8, 2016. http://www.bbc.com/news/technology-36478650*

All is not lost

During the recent Netflix and Spotify attacks[3], hackers were able to exploit vulnerabilities in consumer technology and take control over the behavior of millions of surveillance cameras. The cameras were used to launch a distributed denial of service attack. The same could apply to any connected device. That's the kind of playground that exists for hackers today.

Industrial consumers relying upon cyber security solutions to protect their critical infrastructures have the ability to demand better security requirements for the products they purchase for use in their environments.

In addition, to help mitigate the risk of cyber security incidents, industrial companies can start to behave differently themselves. Too often, industrial companies believe they are isolated from external networks. They believe they are safe because they have no external connections, also known as the air gap. The problem with that belief? It's regularly proven to be untrue.

Just because something is designed one way doesn't mean it stays that way. Points of vulnerability can open up at any time, and organizations need to have well-trained people, well-designed practices and processes, and purpose-built technology that provides an automated means to identify what's happening across their entire network and know, for example, when a rogue access point has opened up, or a new actor has entered the network—whether from outside or within.

The wave of needing to connect internal and external systems is here to stay. It's necessary to remain relevant and competitive. That means companies need to be prepared and they need to connect in a secure way. And the first step toward better security—and safety—is knowledge. Assessing and learning the cyber security posture of operations from a people, process, and technology perspective is the key to secure innovation and capturing new opportunities.

LEARN MORE ABOUT GE DIGITAL SITE ASSESSMENTS.

3 *Ben Dipietro, "Crisis of the Week: Dyn's Denial-of-Service Moment, The Wall Street Journal, October 31, 2016.*

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital