The Cyber Scare

By Bryan Virasami

American companies based in China and at home are being attacked by hackers and competitors looking for information to gain an economic, military and scientific advantage.

If it appears that some officials in Washington have adopted a brand new vocabulary each time they speak the words “security” and “China” in the same sentence, they’re not alone. A growing chorus of cyber security experts and analysts – both in the private sector and government – are sounding the alarm about the escalation of Internet-based attacks originating outside the United States, a situation that many characterize as one of the most severe economic and national security challenges facing the country today.

Indeed, U.S. lawmakers, military officials and the White House agree the threat is severe and are scrambling to fight back and implement new techniques to stop attacks that have reportedly already penetrated military computers, retrieved information from private corporations and pose an unknown danger to transportation networks and power grids.

The threat from hackers just a few years ago who stole credit card numbers to make money now seem like an old story when compared to the new sophisticated type of attacks from
“For the market that I work in, which essentially consists of Western multinationals doing R&D and manufacturing in Asia, China has more attacks than other countries…” — Thomas Parenty of Parenty Consulting

foreign hackers or “actors” as experts call them. Cyber attacks are receiving the most attention because of their near invisible, borderless capabilities. But experts warn that in a digital world where companies store all their business records, intellectual property, research and other technology-related information in electronic form, it can take just a memory stick to copy and steal a chemical formulation, drug composition or aerospace secrets and sell them to a competitor.

While there is disagreement if it’s possible to trace an attack to a specific person or determine if the hacker is working for a state, there is a growing consensus among intelligence officials, and security and military experts that foreign actors – with China and Russia most often singled out – are actively looking to find and steal valuable assets. One U.S. government sanctioned report said the target is business information, communication technology, military secrets about marine systems and unmanned aerial vehicles, as well as other technologies in industries expected to see rapid growth such as clean energy, healthcare and pharmaceuticals.

Some wonder if American companies with offices, factories and research centers in China face a greater danger than their headquarters in the U.S. Others ask if all attackers are looking for the same thing. What can CEOs and their IT departments do about it?

Thomas Parenty, president of Hong Kong-based Parenty Consulting who advises Western multinationals across China and Asia about cyber security, said that cyber attacks and ordinary theft of information is a global issue but acknowledged there’s more activity in China.

“For the market that I work in, which essentially consists of Western multinationals doing R&D and manufacturing in Asia, China has more attacks than other countries because right now, there is a lot of manufacturing being done here and a lot of very sophisticated technology is being developed here,” Parenty told Insight during an interview in Shanghai. “It is still the case that many Western multinationals, as a precaution, will only develop some technologies at home.”

The most common form of cyber attacks comes from the “hackivist community,” people who want to “stir up trouble” who can cause harm but are not generally the best hackers around, according to Kent Kedl, the Shanghai-based managing director for Control Risks, a global risk management consultancy whose services include cyber security. They tend to be associated with a movement and want to protest through hacking. The other kinds are what multinationals should avoid.

“The second kind is what is called APTs – advanced persistent threats – which include sovereign threats from a government of some kind,” Kedl said. “They are focused, they’re targeted, they’re
aggressive, they are coming after you – not just kind of a joyride kind of thing.”

Few executives in China are willing to openly discuss the topic out of fear of drawing attention to their company from hackers. But Western security experts with years of China experience said the goals of offline attacks here are the same: to obtain information that will give an economic or scientific advantage.

U.S. companies tend to be the main targets because the country produces the latest and best technology today. While they’re often most at risk, no one is exempt, including small and medium sized firms, government experts say.

The security issue was also raised during an AmCham Shanghai briefing earlier this year following a published news report that said many U.S. executives traveling to China go to extreme measures to avoid being a victim of skilled hackers. There’s no question cyber attacks are a form of crime without borders, and it matters little if the target is in Seattle or Shanghai.

Experts say that most companies who have been attacked may not find out about it for years. And they often will never

What is Phishing?

One report prepared for a U.S. government agency described it this way: “The practice of enticing a victim to visit a website or other online resource with the intention of stealing credentials, financial information such as bank accounts, or credit card numbers. Phishing attacks generally involve an email claiming to come from a trusted entity such as a bank or ecommerce vendor, with a link to a website and the instructions to click the link and take actions once at the website.”

What is Spear Phishing?

According to the same report: “A targeted phishing attack against a select group of victims, usually belonging to a single company, school, industry, etc. ‘Spear phishing’ is commonly used to refer to any targeted email attack, not limited to phishing.”

Cyber Attack Incidents

The US-China Economic and Security Review Commission identified several China-based attacks aimed at foreign entities

Over the years, several serious hacking incidents have been allegedly traced back to China, including some against U.S. government officials. The Office of the National Counterintelligence Executive, in their 2011 report, cited a few incidents that allegedly came from China.

The report cited a 2011 study in which McAfee said an attack they called “Night Dragon” originated from China and targeted oil, energy and petrochemical companies starting in 2009. Employees were victims of “spear phishing, e-mails and network exploitation.” The attackers sought information about “financing of oil and gas field bids and operations.”

The Chinese government was allegedly behind the January 2010 attack against Google, according to VeriSign iDefense, a charge denied by Beijing.

In 2008, U.S. authorities investigated claims, the report said, that Chinese officials "surreptitiously copied the contents of a US government laptop during then-Commerce Secretary Carlos Gutierrez’s visit to China.”

In November 2008, it was reported “Chinese hackers penetrate the White House information system on numerous occasions, penetrating for brief periods before systems are patched.”
figure out where the attacker is located, who is behind it or whether it's a competitor, nation state, organized crime or just an employee.

“When successful, it is a crime that no one sees,” Parenty said. “If you steal a car it’s very obvious that the car is missing. If you steal information, often times you wouldn’t know that it is gone. One thing that’s very consistent about much theft of corporate information is that it will be a long time before companies know it’s gone.”

Several lawmakers in Washington, military officials and former CIA and FBI officials tend to be more direct and have no reservations about blaming China and the government.

Numerous reports by government-funded offices and private think-tanks have recently chronicled the predominance of attacks and the risks they pose to U.S. and other Western nations. Last year, the Office of the National Counterintelligence Executive in a report, “Spies Stealing US Economic Secrets in Cyberspace,” quoted an unspecified 2010 survey of 200 western executives from the gas, power, oil and water industries in which 85 percent said they were aware of “network intrusions” and that they suspected “government-sponsored sabotage and espionage.”

“Chinese actors are the world’s most active and persistent perpetrators of economic espionage,” the report continued. “U.S. private sector firms and cyber security specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC [intelligence community] cannot confirm who was responsible,” according to the report.

The Canadian government said in a 2010 report that 86 percent of all large Canadian companies were attacked.

Internet-based attacks should not be the only thing on the radar. Within China, U.S. companies should be on the lookout for another type of threat: employees and ex-employees.

“The cyber threat is only a part of it,” said Kedl. “Our China practice that investigates intellectual property violations is huge, it’s the largest practice of its kind in our global operations. This is because there are so many companies here with critical intellectual property and the legal environment in China to protect it is not very strong.”

He explained that there’s big money to be made from stealing technology that took its owner years to develop, selling it to a company that will then commercialize it and put it on the market.

Parenty echoed a similar sentiment.

“In my experience over the last decade in working in this area, most intellectual property is not stolen from attacks over the Internet, it is stolen by an employee who actually had legitimate access to that information in order to do their job,” said Parenty. “And they use that information in ways that would be less common in the U.S. because of the lack of legal repercussions. So there’s a big difference there.”

Unlike the U.S., workers caught stealing intellectual property are not likely to be prosecuted under the current legal system, he said.

The motivation

One of the most widely reported cases was made public last year. American Superconductor Corp., which makes computer systems that operate wind turbines, was nearly destroyed after it lost one of its biggest accounts in China due to flagrant IP theft. Workers from the company were investigating a turbine malfunction in the Gobi Desert that resulted in the discovery.

The company, based in Massachusetts, was using their new...
software in the turbine manufactured by China’s Sinovel Wind Group. The software controls the heart of the system. After the workers sent a copy of the software taken from the malfunctioning turbine to their research center in Austria to see what the problem was, they found out the software inside the turbine was an unauthorized copy. In other words, someone copied the software that they were selling to the Chinese company to use in their turbines.

Sinovel had previously purchased large numbers of turbine controllers from the company but in early 2011, the Chinese firm began refusing shipments at its factory in Liaoning province. Sinovel, which was the biggest customer of the U.S. company, completely stopped all purchases in April, 2011. American Superconductor’s stock fell 40 percent in one day and by 84 percent by September, according to Businessweek. The Massachusetts company realized the Chinese company didn’t need them anymore.

Dejan Karabasevic, a Serbian worker at the company’s Austria research center, was promised US$1.5 million for turning over the software to Sinovel and the company found numerous emails between the two parties and even a contract between the two. He’s now serving prison time in Austria. American Superconductor has filed multiple lawsuits against Sinovel asking for US$1.2 billion in damages but it’s unclear if they’ve made progress. The incident was reportedly raised by U.S. officials during Chinese Vice President Xi Jinping’s visit to the U.S.

Parenty said that case is a lesson in poor internal security measures.

“If you look at the core elements, which is somebody inside the company, for financial rewards, gives trade secrets to a competitor. That is a very common scenario. This is the thing that’s interesting, it wasn’t a cyber attack yet it was something where cyber protection could have been relevant because it was a case where an employee had access to sensitive information and there was no control over how he used it or distributed it.”

The information security chief for a top U.S. technology company said since China’s telecommunications infrastructure is owned and operated by the government, the environment is difficult for private companies. The Chinese government
treats information security and national security as the same issue. As a result, regulations created for national security purposes end up affecting businesses.

“That kind of imbalance makes it very difficult to do business whereas in other countries, it’s like ‘OK enterprise, I will leave you alone. You can do whatever you want as long as you’re not interfering with the national agenda,’” said the security expert who spoke on condition he not be identified. “In China, a lot of these things are intermingled. The infrastructure is intertwined with the commercial side and the State are owners of the infrastructure.”

In coming months and years, cyber security could become a major source of friction between the U.S. and China, some experts say. There are currently two pieces of legislation in Washington to counter cyber attacks but they remain controversial due to privacy concerns. But security experts feel that understanding the threat and dealing with it is the best route for private companies.

Given the scope of the problem and all the rhetoric about fighting cyber and computer related espionage, several security experts said they’re amazed how many American companies with operations in China fail to take appropriate steps to protect their intellectual property.

A senior executive based in Shanghai with a U.S. company said cyber threat is “intangible” and since it doesn’t feel like an imminent problem, it often gets placed on the back burner due to competing priorities that require immediate attention. The threat, he said, is always seen as something that happens to other companies.

“And then we go on dealing with more tangible issues – the disgruntled employee, the unexpected plant outage or the quarterly financial performance. So the biggest concern is that we understand the potential damage that could be caused by the threat, but we underestimate the imminence of the threat,” the executive said.

Another concern, security experts say, is that many U.S. executives here feel there’s nothing that can be done about the risks. And a large number who know the risks exists, tend to take the wrong approach by simply duplicating protective measures used in the U.S. without studying the unique China threat, according to Parenty. He said IT specialists need to spend time in China to analyze the unique threats here and create solutions to target those problems.

Q: You said things that work in the U.S. don’t always work here. What do you mean?

Parenty: “One of the biggest problems that I’ve found is U.S. companies who have done a legitimately good job of developing security standards, procedures and technological guidelines, think that because they exist in the U.S., that the people running their operations in China one, know that they exist, two have read them, three have understood them, four care. Simply because you’ve got something that works in the U.S. does not mean that it’s going to automatically or magically work in China.”
Blame game

While many lawmakers have slammed China and called on the Chinese government to investigate attacks traced back here, they’re not prepared to say the government is behind the attacks – at least not publicly. Security experts are also not prepared to single out any specific entity or organization in China with certainty but agree U.S. companies in the technology, aerospace and chemical industries are among the most at risk and feel that China has more reasons to pursue them.

Kenneth Lieberthal and Peter W. Singer wrote in a 42-page Brookings Institution report, “Cybersecurity and U.S.-China Relations,” that despite a “blanket denial” from China, many hold the view that the cyber threat from China has a “large government-directed component.” They said this is based on the fact the attackers seek out specific things: information about decisions that could impact China, technology with a special strategic interest, NASA and military planning and reconnaissance planning.

Senator John Kerry, chairman of the Senate Foreign Relations Committee [D-Massachusetts], told Insight through a spokesperson that he and others see attacks from China as a big threat. He has spoken out about the cyber threat from China on numerous occasions.

“We know we live in a world without borders and the damage a cybersecurity event across the world can have on markets at home,” he said. “So my main concern is that weak enforcement of robust cyberspace protections in China threatens our economic interests, and an inadequate effort on the part of the government to crack down on unauthorized hacking of American firms is an issue in a delicate relationship.”

Asked whether he agrees with some lawmakers and military reports that blame the Chinese government, Kerry said while there is evidence attacks originate in China, he cannot be certain.

“I cannot and would not accuse the Chinese government of sponsoring cyber attacks without open and shut evidence. I don’t have that smoking gun,” Kerry said. “What we do know, though, beyond any doubt, is that cyber attacks on our firms and networks are originating in China and we have every right to demand that the Chinese government help us stop them. If they don’t, it raises a whole other set of questions.”

An earlier incident that placed the spotlight on China and drew sharp responses from lawmakers, involved the U.S. Chamber of Commerce, which represents most of the major companies in the U.S. The organization, based in Washington D.C., was apparently attacked through the Internet and four employees who work with issues related to Asia were targeted. The attack lasted at least six months and an investigation showed that the attackers sought out documents related to trade policy, meeting notes, reports about trips, schedules and

Cyber Security Expert Suggests ‘A Risk-Based Approach’

Kent Kedl, Managing Director of Control Risks, offers his best tips to companies concerned about the security of their company secrets and cyber related crimes

When considering information security, companies first have to consider just what they are trying to protect. Protecting every piece of data to the same high standard will be costly, difficult to implement, and restrict the creativity and collaboration modern companies need to thrive and develop. We recommend that companies take a risk-based approach. The first step is to assess the threat: Who might be after your IP (competitors? organized crime?) and how would they be able to access it (do they have the capability to hack into your systems or access your people?).

The next step is to ask yourself: “so what...even if I lose this data, what impact will that have on my company?” Assess what information is important, what information is critical to achieve business objectives and should be restricted, and understand what is less important and sensitive.

Implementing a document classification system that is aligned with your business priorities is a simple process that will help you identify how different types of information should be secured and who should have access to them.
“U.S. private sector firms and cyber security specialists have reported an onslaught of computer network intrusions that have originated in China…”

names of certain members, according to published reports of the incident.

The Chamber has 3 million members and said publicly that just about 50 members were affected by the attack but they’re not aware of any loss by members. Some lawmakers said they were concerned that confidential emails between themselves and the Chamber about policy issues were stolen.

Phishing for trouble

The attack against the Chamber apparently utilized what experts call spear phishing, a specialized technique that uses email attachments that look genuine to even the most careful observers. Once opened, the attachment exploits the computer and the command and control servers with malware, according to Parenty, the consultant.

The attackers design the email and attachments for specific targets and the emails always contain information the recipients expect, Parenty said. The attackers may spend months, sometimes years, preparing an attack designed to obtain large amounts of information undetected.

Spear phishing is also unique in that emails are designed to look normal and come from people the recipients know and trust. It could be a schedule to an upcoming conference that the victim has signed up for and the attackers know about due to their monitoring.

“The old advice that you would give of ‘Oh don’t open suspicious attachments; doesn’t work here because it won’t look suspicious,” Parenty said. “It will look exactly like something that you should be getting. It’s customized for you, so to you should feel special.”

Fighting back

The White House, lawmakers, the military and private security consultants have all expressed a desire to attack the problem more aggressively but there is little consensus. President Obama is often quoted as saying that the cyber threat is “one of the most serious economic and national security challenges we face as a nation.” He has appointed a cyber security coordinator and is working with various government and civilian bodies to assess and counter the problem.

In addition, several lawmakers have been critical of China. Rep. Mike Rogers, chairman of the House Intelligence Committee, for example, has called for the U.S. to approach the problem as a bilateral trade issue with China because in his opinion intellectual property theft results in the loss of jobs for Americans.

Both the House and Senate have bills that would require more sharing of information between the private sector and government. Opponents said the bills could hurt civil liberties and privacy. President Obama has threatened to veto the House bill and has expressed support for the Senate version but the body is divided over that bill.

“There is an economic cyber war going on today against U.S. companies,” Rogers, who co-sponsored the Cyber Intelligence Sharing and Protection Act, told reporters in a statement. “Economic predators, including nation-states, are blatantly stealing business secrets and innovation from private companies.”

Technology is only part of the solution – and while it should be developed in layers with multiple vendors and regular updates and audits, remember that even the best systems in the world can be thwarted by more sophisticated technology or by the willingness of an unwitting colleague to share information: in the hotel lobby, in the elevator, on the airplane, carelessly leaving documents on the printer or ignoring the clean desk policy, etc.

Make sure your employees understand the danger of opening unknown attachments or clicking on unknown links, and remain vigilant against attempts to pry into company business by unauthorized employees, strangers, suppliers, vendors and competitors. A regular training and awareness program should accompany policies and procedures that are reviewed and respond to the changing risk environment.

For those employees who have access to critical information, but need to travel, consider taking “clean” electronic devices. Make sure you keep electronic and hard copy files on you at all times, don’t even assume the hotel safe is secure. Avoid connecting to wireless networks, change your passwords frequently and have your IT department check you device when you return.