EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008. Chelmsford. MA 01824

February 15, 2017 - Volume 9, Issue 4

CBP, ICE Seize Record Number of Shipments with Intellectual Property Rights Violations in FY2016

Release Date:
January 13, 2017

Seized goods would have been worth more than $1.38 billion if genuine

WASHINGTON – U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) seized a record number of shipments containing goods that violated Intellectual Property Rights (IPR) in FY2016. The number of IPR seizures increased **9 percent** in FY2016 to more than **31,560**. The total estimated manufacturer's suggested retail price (MSRP) of the seized goods, had they been genuine, increased to more than **$1.38 billion**. As a result of enforcement efforts, ICE Homeland Security Investigations arrested **451** individuals, obtained **304** indictments, and received **272** convictions related to intellectual property crimes in FY2016.

The People's Republic of China remained the primary source economy for counterfeit and pirated goods seized, accounting for **$616 million** or **45 percent** of the total estimated MSRP value of all IPR seizures. Hong Kong again was the second largest source of IPR infringing shipments, accounting for nearly **$600 million** or **43 percent** of the total MSRP value of all IPR seizures.

NEWSLETTER NOTES

NIAR joins NASA-led group to advance aviation composites

BY JERRY SIEBENMARK
jsiebenmark@wichitaeagle.com

A public-private effort launched by NASA to bolster knowledge of composite materials and improve aircraft performance now includes Wichita State University's National Institute for Aviation Research.

NIAR has joined NASA's Advanced Composite Consortium, which includes the Federal Aviation Administration, Boeing, GE Aviation and Orbital ATK. The consortium aims to decrease product development and certification times for composites used in aeronautics, according to a WSU news release on Tuesday.

"Our experience and understanding of composite material properties and certification processes will add to the already strong intellectual membership," said Royal Lovingfoss, associate director of NIAR's Composites and Advanced Materials Lab. "The collaborative experience will bring new ideas to the forefront and allow for a sharing of information that will benefit the aviation community as a whole."

Climate Change and Robotics

Recently, scientists reported that the Earth reached its highest temperature on record in 2016, trouncing a record set only a year earlier, which beat one set in 2014. It is the first time in the modern era of global warming data that temperatures have blown past the previous record three years in a row (below).

In the United States alone there are over 3,500 landfills that emit 20% of dangerous methane gas into the atmosphere. Since 1960, humans have doubled the daily garbage contribution due to our thirst for plastic water bottles. Just last year, Americans used about 50 billion plastic water bottles, with 80% ending up in landfills. This means that 38 billion water bottles or $1 billion worth of recycled materials are wasted every year. Most of the world's recycling plants cannot afford large industrial spectrometers to sort garbage, and rely on inefficient, expensive, human labor……..

Watch the video below:

https://youtu.be/hUKNTaPQwBc

BIS Articles

1/19/17
82 FR 6218

Amendments to the Export Administration Regulations Implementing an Additional Phase of India-U.S. Export Control Cooperation

In this final rule, the Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) to implement the India–U.S. Joint Statement of June 7, 2016 (June Statement), which recognized the United States and India as Major Defense Partners. This rule amends the EAR by establishing a licensing policy of general approval for exports or reexports to or transfers within India of items subject to the EAR and controlled only for National Security or Regional Stability reasons. In addition, BIS amends the end use and end user provisions of the Validated End User (VEU) authorization to state that items obtained under authorization VEU in India may be used for either civil or military end uses other than those that are for use in nuclear, "missile," or chemical or biological weapons activities.

1/19/17
82 FR 6216

Support Document Requirements With Respect to Hong Kong

This rule requires persons intending to export or reexport to Hong Kong any item subject to the Export Administration Regulations (EAR) and controlled on the Commerce Control List (CCL) for national security (NS), missile technology (MT), nuclear nonproliferation (NP column 1), or chemical and biological weapons (CB) reasons to obtain, prior to such export or reexport, a copy of a Hong Kong import license or a written statement from the Hong Kong government that such a license is not required. This rule also requires persons intending to reexport from Hong Kong any item subject to the EAR and controlled for NS, MT, NP column 1, or CB reasons to obtain a Hong Kong export license or a statement from the Hong Kong government that such a license is not required. The rule is effective on April 19, 2017.

Aviation Week Network Selects Top 20 Aerospace-Bound Engineering Students

NEWS PROVIDED BY
Aviation Week Network
Jan 12, 2017, 09:00 ET

NEW YORK, Jan. 12, 2017 /PRNewswire/ -- Aviation Week Network (http://www.aviationweek.com), in collaboration with the American Institute of Aeronautics and Astronautics (AIAA), announced today the winners of its awards program, "Tomorrow's Engineering Leaders: The 20 Twenties."

The awards recognize top science, technology, engineering, and math undergraduate and graduate students. The program connects the next generation of aerospace and defense talent with established innovators and leaders honored at the Laureates Awards, who have created many of the "firsts" driving innovation in the 21st century.

"One of the pillars of our service to the aerospace community is actively engaging and developing next-generation technology talent who are essential to the future of this exceptional industry," Greg Hamilton, Aviation Week Network president, said. "Truly, this year's nominees and winners represent the best in terms of their talent, their creativity, and ability."

"The winners for this year's 20 Twenties program reflect the diversity, ingenuity and remarkable talent found within the aerospace community," said Sandy Magnus, AIAA executive director. "Each of these outstanding students, from around the world, is making significant contributions to their fields of study – ranging from electric propulsion to hypersonics to autonomous vehicles – as well as working to make the world a better place. Their research is shaping not only the future of aerospace, but the future of humanity, and each is uniquely worthy of our praise and this honor."

This year's recognition program had qualified nominees from 36 different universities. The winners will be honored during Aviation Week's 60th Annual Laureates Awards March 2 at the National Building Museum, Washington, DC. The 2017 20 Twenties winners are:

*(*Continued On The Following Column)*

-Keenan E. S. Albee, Columbia University

-Geoffrey Andrews, Purdue University

-Jakob Bludau, Technical University of Munich

-Julia CrowleyFarenga, Purdue University

-John L. Deaton, U.S. Air Force Academy

-Julia Di, Columbia University

-Jennifer Domanowski, Boise State University

-Karl Domjahn, The University of Queensland

-Alexander W. Feldstein, Massachusetts Institute of Technology

-Brian Free, University of Maryland

-Kelly Henckel, University of Michigan

-Rebecca E. Hill, University of Michigan

-Matthew Ryan Hurst, University of Colorado, Boulder

-Rubbel Kumar, University of Maryland

-Braven C. Leung, Georgia Institute of Technology

-Wanyi Ng, University of Maryland

-Kristen Railey, Massachusetts Institute of Technology

-Christine Reilly, University of Colorado, Boulder

-Rose Weinstein, University of Maryland

-Emily Marie Zimovan, Purdue University

For more information about 20 Twenties Awards, please contact Carole Hedden at Carole.Hedden@AviationWeek.com

7 best encrypted messaging apps for all the Edward Snowdens out there

Love him or hate him, Edward Snowden made many of us more aware.

We now pay close attention to our online privacy and care about things like metadata, surveillance, digital snooping, and data theft. While governments and companies wage war about how much of our information should be accessible in different situations, app developers are giving us the tools to decide for ourselves what we want to share.

They're creating encrypted services and launching end-to-end encryption options we can enable in apps. With these tools, we're able to make sure that only us - and the people we're communicating with - can read what is sent. Nobody in between, not the government nor even the companies and developers offering these tools, can access it.

Many different departments and police agencies prefer to have access to all our communications in order to stop criminals, and because of that, end-to-end encrypted services, which again means only the sender and the recipient are able to read messages, are hotly debated. But privacy campaigners warn that undermining encryption is a rights violation.

Sometimes encryption happens automatically, so there's no need to turn on a setting. Other times, it's trickier. You may even need to set up secret chats. In the post-Snowden era, you can never be too concerned about your privacy. With that in mind, here are some of the best encrypted messaging apps available now for Android and iOS devices.

Best encrypted messaging apps

In alphabetical order:

Facebook Messenger
Download: Android (free) | iOS (free)

Facebook Messenger barely made this list, because technically, it isn't fully end-to-end encrypted. We only included it because it's the world's most popular messaging app, and it does actually offer an optional end-to-end encryption feature, called Secret Conversation, which you can enable for individual chat conversations from an Android or iOS device (it's not yet available for desktops).

*(*Continued On The Following Column)*

Messages sent using end-to-end encryption won't support GIFs, calls, or videos, but Facebook users will be able to set timers on messages, enabling the threads to self-destruct after a set amount of time, sort of like Snapchat Snaps. Messenger's encryption is also based on Open Whisper System's Signal Protocol, which is whistleblower Snowden's preferred means of encryption.

Facebook said both you and the other person in the secret conversation have a device key that you can use to verify that the messages are end-to-end encrypted. The feature only works from one phone, tablet, or computer. Keep in mind that the person you're messaging could still choose to share the conversation with others via a screenshot. To learn more, check out Facebook's Help Center.

Signal
Download: Android (free) | iOS (free)

Open Whisper Systems' Signal is probably the best-known messaging app for mobile users concerned about their privacy. It is a free app that provides messaging and voice-call services - and everything is completely end-to-end encrypted. You can send text messages to individuals and groups, place calls, share media and other attachments to your phone contacts, and more.

The best part is you don't have to use PIN codes or generate special logins. Messages can also self-destruct after a set amount of time. And if you want to use Signal from your computer, there's a new Chrome browser plugin for desktops.

Silent
Download: Android ($9.95/mo) | iOS ($9.95/mo)

Silent Circle is another trusted solution that provides not only secure-communications software but also hardware like the Blackphone. The company's mobile-messaging platform, Silent Phone, offers encrypted, self-destructing messages and file transfers as well as encrypted video and voice calls. You hold the encryption key, not Silent Circle, so while your data does pass through Silent Circle's network, it can't read anything. Unfortunately, you must be a paid subscriber to use the app.

Telegram Messenger
Download: Android (free) | iOS (free)

Telegram Messenger is one of the more user-friendly solutions - and it's marketed as the "fastest". Just link your Telegram account to your phone number, and you can use the app to send encrypted chat messages over the cloud. You can even set message to self-destruct. Everything on Telegram, including chats, groups, media, etc, is encrypted. It also includes fun photo- and video-editing tools, as well as a sticker/GIF platform so you can get creative with your chats.

(*Continued On The Following Page)

WhatsApp
Download: Android (free) | iOS (free)

WhatsApp slowly rolled out its end-to-end encryption offering. It first partnered with Open Whisper Systems in 2014 to add the same encryption methods used in Signal, and then in 2016, it announced that all WhatsApp communications - voice messages, photos, video messages, chats, group chats, etc - are protected by end-to-end encryption. It even provides a security-verification code that you can share with a contact to ensure that your conversation is encrypted.

Wickr Me
Download: Android (free) | iOS (free)

Wickr Me is a lesser-known end-to-end encrypted-messaging app, but it works much like the others. You can send private, self-destructing messages, photos, video, and voice messages to other Wickr contacts. It also deletes metadata like geotags and message times. Plus, there's a
"Secure Shredder" feature that enables you to securely erase attached files, messages, and other data should someone try to recover anything.

Viber
Download: Android (free) | iOS (free)

Viber recently joined the end-to-end encryption crowd. It's unique in that it sports a colour-coded system that show how protected your conversations are with a person. Grey means encrypted communications, green means encrypted communications with a trusted contact, and red means there is an problem with the authentication key. Viber can also hide chatrooms on a shared device. And everything, from text to voice messaging, is tied to your number. But if you want to call non-Viber users, you'll have to pay up.

Worth mentioning
iMessage: Apple's default messaging app is also encrypted, but encryption experts have noted iMessage uses an Apple-developed encryption that doesn't follow all of the best practices. You can't verify contacts' identities, for instance, and the code isn't open to independent review. Also, an exploit was recently found that would allow a sophisticated attacker to decrypt photos and videos sent over the service. Still, Apple couldn't read the messages even if they were ordered to by a court order, so that's nice.

U.S. Army, GM Team Up to Build Fuel Cell Vehicle

The ZH2 is an electric car that uses fuel cell technology and was unveiled at a DC auto show.

BY KEN-YON HARDY, STARS AND STRIPES / JANUARY 27, 2017

USARMY/DAVID VERGUN
(TNS) -- WASHINGTON — The ZH2 fuel cell electric vehicle, developed and built by General Motors for the U.S. Army to test and evaluate the readiness of fuel-cell propulsion in military-like environments, is in the public eye this week at the Washington Auto Show.

Representatives of of GM and the Army's Tank Automotive Research, Development and Engineering Center (TARDEC) met with reporters at the Walter E. Washington Convention Center on Thursday to show off the new technology.

"Our engineers and scientists are excited about the soldiers' feedback on their experience using a fuel cell vehicle," said TARDEC Director Dr. Paul Rogers. "Ultimately these warfighters are our customer, and bringing their vehicles the capabilities that make their missions successful and bring them home safely is paramount."

RELATED

Hydrogen-Cell Bus Debuts at Columbus, Ohio, Statehouse
Oakland Expo Showcases Alternative Fuel Vehicles
Connecticut to Expand Its Fuel Cell Industry
The ZH2, a version of the Chevrolet Colorado mid-size truck, will be on display for the duration of the show from Jan. 27 through Feb 5.

Senate confirms former Exxon CEO Rex Tillerson as secretary of state

Rex Tillerson won confirmation Wednesday to become secretary of state, placing a lifelong oil company executive at the helm off what President Trump has promised will be an “America first” foreign policy.

Tillerson takes office after a chaotic first few weeks for the Trump administration that saw big swings away from the national security and foreign policy policies in place under the Obama administration.

The State Department he now heads has a central role in refugee resettlement and other immigration and travel-related policies now at issue in a White House order suspending the admission of refugees and restricting entry for citizens from several Muslim-majority nations.

He also is head of Defense Trade Office which overseas licensing or Military Goods, Technical Data and Services around the globe.

OFAC

Publication of Kingpin Act/Panama-related General License

2/1/2017
Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published two Kingpin Act General Licenses: General License 5C, "Authorizing Certain Transactions and Activities Related to the Panamanian Government Seizure of Balboa Bank & Trust", and General License 6C, "Authorizing Certain Transactions and Activities Related to the Intervention by the Superintendency of Securities Markets of Panama in Balboa Securities, Corp." These licenses extend existing authorizations regarding certain transactions and activities that would otherwise be prohibited pursuant to the Kingpin Act. Both authorizations expire on April 7, 2017, unless extended or revoked.

Amendment to Publication of Kingpin Act/Panama-related General License

2/2/2017
The notice "Kingpin Act/Panama-related General License" was amended on February 2, 2017 to read as follows:

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published two Kingpin Act General Licenses: General License 5C, "Authorizing Certain Transactions and Activities Related to the Panamanian Government Seizure of Balboa Bank & Trust", and General License 6C, "Authorizing Certain Transactions and Activities Related to the Intervention by the Superintendency of Securities Markets of Panama in Balboa Securities, Corp." These licenses extend existing authorizations regarding certain transactions and activities that would otherwise be prohibited pursuant to the Kingpin Act. Both authorizations expire on April 7, 2017, unless extended or revoked. OFAC is also amending two Frequently Asked Questions.

Update to the Iranian Transactions and Sanctions Regulations, 31 CFR Part 560, Section 560.530(a)(3), List of Medical Devices Requiring Specific Authorization

2/2/2017
The Department of the Treasury's Office of Foreign Assets Control (OFAC) is updating the List of Medical Devices Requiring Specific Authorization as identified in 31 C.F.R. § 560.530(a)(3)(ii) of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR), to update and clarify the scope of medical devices that are not authorized for exportation or reexportation pursuant to the general license at 31 C.F.R. § 560.530(a)(3)(i).

*(*Continued On The Following Page)*

For reference, OFAC previously published related frequently asked questions on the general license to provide guidance on the scope and limitations of this general license.

Publication of Cyber-related General License

2/2/2017
Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) published Cyber-related General License (GL) 1, "Authorizing Certain Transactions with the Federal Security Service," pursuant to Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." GL 1 authorizes certain transactions with the Federal Security Service (a.k.a. FSB) that are necessary and ordinarily incident to requesting certain licenses and authorizations for the importation, distribution, or use of certain information technology products in the Russian Federation, as well as transactions necessary and ordinarily incident to comply with rules and regulations administered by, and certain actions or investigations involving, the FSB.

Market Forecast indicates Military UAV market to grow with CAGR of 38.7%

The global military UAV market is projected to grow to USD 13.9 billion by 2026, at a CAGR of 38.7% from 2016 to 2022. Where the MUAV/MAVs are dominant in terms of units delivered and the UCAVs in terms value.

In recent years, there has been a growing use by militaries around the world of Unmanned Aerial Vehicles, more popularly known as drones. More than 10,000 UAVs are now operated or coming into service with militaries around the world. Their increased usage has mostly been driven by the operational experience of the US and Israel, as well as recent operations in Afghanistan, Iraq and Syria for intelligence, surveillance and reconnaissance (ISR) tasks with the US leading the way in terms of spending on research, procurement and support. Other countries are gaining and developing their own platforms in part to enhance their military intelligence capabilities, or as some exercise in national prestige to develop their own defense and aerospace industries.

U.S. Nuclear Engineer Pleads Guilty to Violating the Atomic Energy Act

Szuhsiung Ho, aka Allen Ho, 66, a naturalized U.S. citizen, pleaded guilty to conspiracy to unlawfully engage or participate in the production or development of special nuclear material outside the U.S., without the required authorization from the U.S. Department of Energy (DOE) in violation of the Atomic Energy Act. Acting Assistant Attorney General for National Security Mary B. McCord and U.S. Attorney Nancy Stallard Harr of the Eastern District of Tennessee made the announcement.

In April 2016, a federal grand jury issued a two-count indictment against Ho; China General Nuclear Power Company (CGNPC), the largest nuclear power company in China, and Energy Technology International (ETI), a Delaware corporation. At the time of the indictment Ho was a nuclear engineer, employed as a consultant by CGNPC and was also the owner of ETI. CGNPC specialized in the development and manufacture of nuclear reactors and was controlled by China's State-Owned Assets Supervision and Administration Commission.

According to documents filed in the case, beginning in 1997 and continuing through April 2016, Ho conspired with others to engage or participate in the development or production of special nuclear material in China, without specific authorization to do so from the U.S. Secretary of Energy, as required by law. Ho assisted CGNPC in procuring U.S.-based nuclear engineers to assist CGNPC and its subsidiaries with designing and manufacturing certain components for nuclear reactors more quickly by reducing the time and financial costs of research and development of nuclear technology. In particular, Ho sought technical assistance related to CGNPC's Small Modular Reactor Program; CGNPC's Advanced Fuel Assembly Program; CGNPC's Fixed In-Core Detector System; and verification and validation of nuclear reactor-related computer codes.

Under the direction of CGNPC, Ho also identified, recruited, and executed contracts with U.S.-based experts from the civil nuclear industry who provided technical assistance related to the development and production of special nuclear material for CGNPC in China. Ho and CGNPC also facilitated the travel to China and payments to the U.S.-based experts in exchange for their services.

*(*Continued On The Following Page)*

Sentencing has been set for May 17, 2017, at 11:00 a.m., in U.S. District Court in Knoxville, Tennessee. Ho faces a maximum sentence of 10 years in prison and a maximum $250,000 fine. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes, as the sentencing of the defendant will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

This case was investigated by the FBI, Tennessee Valley Authority-Office of the Inspector General, DOE-National Nuclear Security Administration and U.S. Immigration and Customs Enforcement Homeland Security Investigations, with assistance from other agencies. Assistant U.S. Attorneys Charles E. Atchley Jr. and Bart Slabbekorn of the Eastern District of Tennessee, and Trial Attorney Casey T. Arrowood of the Counterintelligence and Export Control Section and Attorney Jeffrey M. Smith of the Appellate Unit in the National Security Division, represented the U.S.

CYBER, HACKING, DATA THEFT, COMPUTER INTRUSIONS & RELATED
Ransomware: Now a Billion Dollar a Year Crime and Growing

Ransomware payments for 2016 are expected to hit a billion dollars, according to the FBI. That compares to just $24 million paid in 2015.

And it's expected to get even worse this year — with more victims and more money lost.

Experts even predict that the cloud could come under attack this year because it's such a lucrative target and could result in ransom payments in the millions of dollars.

Ransomware is a family of malware that blocks access to a PC, server or mobile device, or encrypts all the data stored on that machine. It's typically delivered via malicious email or infected third-party websites.

To regain access or control of the data, the user must pay a ransom — typically via bitcoin. The encryption is unbreakable and simply removing the malware will not solve the problem. The victim is forced to pay for the unique software key that will unlock everything.

"It's like some sort of gold rush," said Limor Kessem, executive security adviser for IBM Security. "Cybercriminals are using ransomware to bring extortion to the masses and more criminals are now doing it because they're interested in getting a piece of the action."

*(*Continued On The Following Column)*

The average ransom demanded in 2016 was $679, more than double the $295 demanded at the end of 2015, according to a report from Symantec. Some businesses that experience a ransomware attack are making 4- to 5-digit payments to get their data unlocked.

"We did a survey in the U.S. and discovered that 64 percent of end users who got ransomware paid the ransom," said Kevin Haley, director of Symantec Security Response. "People are willing to pay, so the bad guys keep raising the price. We'll probably see it hit a thousand dollars before 2017 is over." Criminal gangs are now capable of pushing their malware to millions of computers a day. In fact, Malwarebytes reports that 60 percent of all malware observed last year was ransomware. Not everyone gets infected, but a lot do.

"It's a fantastic money maker," said Adam Kujawa, director of malware Intelligence for Malwarebytes.

"With other types of malware, a criminal has to deal with collecting personal information like passwords or credit card numbers and then try to resell that in the underground marketplace to other criminals," he said. "With ransomware, it's direct. You infect someone, they pay you directly."

It's Going to Get Much Worse

Digital security experts tell NBC News the number of ransomware attacks skyrocketed in 2016 and the sophistication of this malware grew exponentially. And they say it's going to get worse.

More criminals are expected to shift to ransomware because they can now buy ready-made ransomware software from super hackers. These toolkits make it possible for anyone with basic computer skills to launch sophisticated attacks.

The menace will also grow as new variants of this malicious software are developed that do more than simply encrypt the data. For example, "Jigsaw" encrypts the data and then starts deleting groups of files to put pressure on the victim to pay up quickly. "Chimera" threatens to post the victim's files online, including pictures and videos, if the ransom is not paid by the deadline.

We may also see attacks on devices that use the Android operating system. Symantec has already discovered ransomware called "Flocker" that can lock Android smart TVs.

With ransomware, the criminals can be anywhere in the world and attack any individual or corporate computer connected to the Internet. A survey by Symantec found that the U.S. was the favorite target with 28 percent of global infections. Canada was a distant second at 16 percent.

(*Continued On The Following Page)

Right now, individual computer users are the most likely victims because they tend to have less robust security in place. But as we saw last year, corporate systems are also vulnerable. It's been reported that hospitals, police departments, colleges, banks, and utilities paid a ransom in order to regain access to their information.

In February, Hollywood Presbyterian Medical Center in Los Angeles paid nearly $17,000 to unlock the hospital's computer network. "The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," hospital CEO, Allen Stefanek said in a statement at the time.

In late November, ransomware hit the San Francisco Municipal Transportation Agency and disabled the ticket vending machines for Muni light rail.

The Symantec report warns that some ransomware gangs are increasingly interested in hitting businesses and that they're using "advance attack techniques, displaying a level of expertise similar to that seen in many cyber espionage attacks." Businesses are more likely to pay the ransom if they don't have backup files and can't get things up and running again quickly.

Would You Pay to Get Your Files Back?

IBM asked 600 U.S. business leaders what they would do if they faced this sort of extortion. The survey results show 70 percent of the businesses infected with ransomware had paid a ransom to regain access to their business data and systems. Half of these companies paid more than $10,000 and 20 percent paid more than $40,000. Other key findings:

· Nearly half of the executives surveyed said their company had experienced a ransomware attack

· Nearly 60 percent indicated they would pay a ransom to recover data

· Twenty-five percent said they'd be willing to pay between $20,000 and $50,000, depending on the type of data lost.

Limor Kessem, who wrote the IBM Security report, told NBC News she was surprised to learn how many businesses had already experienced a ransomware attack.

Ransomware is pretty much the only malware that can impede everything you're doing," Kessem said. "It can lock up your devices altogether or it can lock up the data on those devices. And this can paralyze a business."

Law enforcement discourages victims from paying the ransom — believing it encourages more attacks and pays for the development of more evil malware. There's also no guarantee that once the ransom is paid, the files will be unlocked. But many businesses pay because they're not prepared and feel they have no other option.

*(*Continued On The Following Column)*

Anyone hit by ransomware should file a report via the FBI's Internet Crime Complaint Center. The FBI also has tips for protecting yourself and your organization.

Big and medium-sized companies are more attractive extortion victims, since they can pay a bigger ransom. But the IBM report cautions small businesses that they remain "a ripe target" for ransomware because their employees often lack training in workplace IT security. The study found that only 30 percent of the 200 small businesses surveyed offer security training to their employees, compared to 58 percent of larger companies.

Everyone Is at Risk

Everyone who goes online — via home computer or mobile device — needs to be prepared for a ransomware attack and take steps to reduce the chances of infection.

And while you may say you'd never pay if you got hit — you might reconsider if all of your financial files, family pictures or everything stored on your mobile phone are locked and you don't have backups anywhere.

"You have to prepare for it now. You have to arm yourself and put proper security precautions in place because if you don't protect your files, nobody else will," said Malwarebytes Adam Kujawa. "You need to think of it as being in a war and you need to protect yourself."

As part of its just-released survey, IBM asked more than a thousand American adults about ransomware. Only one-third had heard of it and 59 percent had not taken any proactive measures in the past three months to protect their devices from being hacked.

How to Protect Yourself

Think before you click

Most ransomware is delivered via email that tells you to click on a link or open an attachment. The message is designed to get you to open that infected attachment. It could appear to be information about a package delivery or an invoice that you're supposed to pay. If you're not expecting it, don't open it. IBM found that nearly 40 percent of all spam emails sent in 2016 contained ransomware.

Back up all of your data

You should have a frequent and regular backup routine for all of your devices no matter which operating system they use. Apple software is not immune. Symantec reports that in March of 2016, "KeRanger" became the first widespread ransomware to target the Mac OS X operating system. You can back up in the cloud, on a thumb drive or external drive. Just make sure your backups are secure and not constantly connected or mapped to the live network or they could also get infected.

*(*Continued On The Following Page)*

Update, patch and purge

You should be set to receive automatic updates for all software, including operating systems, apps and security software — on all devices. Delete any applications that you rarely or never use.

Disable those macros

IBM reports that document macros are now a common way to deliver ransomware. That's why macros for email and documents should be disabled by default.

"This is not something that happens to other people, it could easily happen to you," cautioned Symantec's Kevin Haley. "We really need to step up our protection because the bad guys are stepping up their game. There's just too much money involved for them not to."

Chinese National Admits to Stealing Sensitive Military Program Documents from United Technologies

Yu Long, 38, a citizen of China and lawful permanent resident of the U.S., waived his right to be indicted and pleaded guilty today in New Haven federal court in Connecticut, to charges related to his theft of numerous sensitive military program documents from United Technologies and transporting them to China.

Long pleaded guilty to one count of conspiracy to engage in the theft of trade secrets knowing that the offense would benefit a foreign government, foreign instrumentality or foreign agent, an offense that carries a maximum term of imprisonment of 15 years. He also pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S. in violation of the Arms Export Control Act, an offense that carries a maximum term of imprisonment of 20 years. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendant will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors. The announcement was made by Acting Assistant Attorney General for National Security Mary B. McCord, U.S. Attorney Deirdre M. Daly for the District of Connecticut, Special Agent in Charge Matthew Etre of the FBI's Homeland Security Investigations (HSI) in Boston, Massachusetts, Special Agent in Charge Craig W. Rupert of the Defense Criminal Investigative Service (DCIS) Northeast Field Office, Special Agent in Charge Patricia M. Ferrick of the FBI's New Haven Division and Special Agent in Charge Danielle Angley with the Air Force Office of Special Investigations (AFOSI).

*(*Continued On The Following Column)*

"Long admitted to stealing and exploiting highly sensitive military technology and documents, knowing his theft would benefit China's defense industry and deliberately contravene the embargo on U.S. Munitions List technology the United States has imposed on China," said Acting Assistant Attorney General McCord. "Export laws exist as an important part of our national security framework and disrupting and prosecuting this kind of economic espionage is one of the National Security Division's highest priorities."

"In an effort to further his own career, this defendant stole an extraordinary amount of proprietary military program information from United Technologies and transported much of that stolen information to China," said U.S. Attorney Daly. "His actions, which he knew would benefit China, not only violated his employment agreement and damaged the company, but have threatened our country's national security interests. U.S. companies continue to be targeted by those who seek to steal intellectual property, trade secrets and advanced defense technology – whether through a computer hack or cyber intrusion, or through a rogue employee. Working closely with our nation's defense contractors, we will relentlessly investigate and prosecute those who steal, or attempt to steal, trade secrets and sensitive military information, whether for their own personal gain or for the benefit of foreign actors."

"These sophisticated technologies are highly sought after by our adversaries," said Special Agent in Charge Etre. "They were developed to give the United States and its allies a distinct military advantage, which is why HSI and our law enforcement partners will continue to aggressively target the individuals who steal the ideas of others and sell these items." "Today's plea demonstrates the commitment of the Defense Criminal Investigative Service and our federal law enforcement partners to identifying those who illegally export sensitive defense information to adversarial Foreign governments," said Special Agent in Charge Rupert. "DCIS will continue to safeguard sensitive technology and to shield America's investment in national defense by disrupting efforts of groups and individuals who try to illegally acquire our national security assets."

"This case highlights the complexity in which the FBI and law enforcement are being challenged to keep the integrity of our industry intellectual property intact," said Special Agent in Charge Ferrick. "Investigating criminal activity of this nature will continue to be a priority."

"This case was enabled by the outstanding teamwork of the FBI, DCIS, HSI, AFOSI and the U.S. Attorney's office," said, Special Agent in Charge Angley. "In addition, it demonstrates the focus of law enforcement agencies to protect our nation's critical resources."

(*Continued On The Following Page)

According to court documents and statements made in court, from approximately May 2008 to May 2014, Long worked as a Senior Engineer/Scientist at United Technologies Research Center (UTRC) in Connecticut. Long's employment at UTRC included work on F119 and F135 engines. The F119 engine is employed by the U.S. Air Force F-22 Raptor fighter aircraft, and the F135 engine is employed by the U.S. Air Force F-35 Lightning II fighter aircraft.

Beginning in 2013, Long expressed his intent to individuals outside UTRC to return to China to work on research projects at certain state-run universities in China using knowledge and materials he had acquired while employed at the UTRC. To that end, Long interacted with several state-run institutions in China, including the Chinese Academy of Science (CAS) and the Shenyang Institute of Automation (SIA), a state-run university in China affiliated with CAS.

During 2013 and 2014, Long was recruited by SIA and other state-run universities, during which he leveraged information that he had obtained while working at UTRC to seek employment in China, culminating in his travel to China in the possession of voluminous documents and data containing highly sensitive intellectual property, trade secrets and export controlled technology, which he had unlawfully stolen from UTRC.

In December 2013, after Long agreed in principle to join SIA, an SIA-CAS Director and an SIA-CAS Recruiter asked Long to provide documents from his work at UTRC and examples of projects on which he had worked to substantiate the claims Long made in his application, and interview with SIA. Long agreed.

On Dec. 24, 2013, Long emailed several documents to the SIA-CAS Director, including a document that contained the cover page of an export controlled UTRC presentation on Distortion Modeling dated Sept. 30, 2011.

While negotiating with SIA, Long also continued to explore other opportunities at other state-run institutions in China. In one email, Long stated: "I have made my mind to return to China, so have prepared a research plan based on my industry experience and current projects." In the research plan, Long stated: "In the past five years, I have been working with Pratt Whitney, also other UTC business units, like UTAS (including Hamilton Sundstrand and Goodrich), Sikorsky, CCS (including Carrier and Fire & Security), and Otis. These unique working experiences have provided me a great starting point to perform R&D and further spin off business in China. I believe my efforts will help China to mature its own aircraft engines." On May 30, 2014, Long left UTRC. In June 2014, Long traveled to China and began working for SIA.

*(*Continued On The Following Column)*

Beginning in July 2014, digital evidence and forensic analysis indicated that Long brought with him and accessed in China a UTRC external hard drive that had been issued to him and that he unlawfully retained.

In July 2014, Long was listed as the project leader on a lengthy research plan for CAS involving fourteen other individuals. The plan was replete with references to how the proposed research and development would benefit China. The plan stated: "The three major engine companies in the world, i.e. GE, Pratt & Whitney in the US and Rolls-Royce in the UK, are all using this technology. . . Our nation lacks the ability to process high performance components, such as airplane wings, tail hooks on carrier aircrafts, and blisks . . . Because of the technology embargo imposed by western developed countries, it is very difficult for us to obtain more advanced design and manufacturing technology . . . This research project will increase our independent ability, efficient and quality in key component manufacturing."

On or about Aug. 12, 2014, the document on Distortion Modeling – the same document from which Long had sent the cover page to the SIA-CAS Director on Dec. 24, 2013 – was accessed on the external hard drive. Travel records and forensic analysis confirmed that both Long and the external hard drive were in China when this file was accessed.
On Aug. 19, 2014, Long returned to the U.S. from China through John F. Kennedy International Airport in New York. During a secondary inspection screening by U.S. Customs and Border Protection (CBP) officers, Long was found in the possession of a largely completed application for work with a state-controlled aviation and aerospace research center in China. The application highlighted certain parts of Long's work related to the F119 and F135 engines while at UTRC.

On or about Aug. 20, 2014, Long emailed an individual at a university in China, attaching an updated "achievement and future plan." In the plan, Long discussed his work related to the F119 and F135 U.S. military fighter jet engines and stated that he also had knowledge of unpublished UTRC projects in which the U.S. Air Force had shown interest.

On Nov. 5, 2014, Long boarded a flight from Ithaca, New York to Newark Liberty International Airport in Newark, New Jersey, with a final destination of China. During Long's layover in Newark, CBP officers inspected Long's checked baggage and discovered that it contained sensitive, proprietary and export controlled documents from another defense contractor, Rolls Royce.

Further investigation determined that the U.S. Air Force had convened a consortium of major defense contractors, including Pratt and Rolls Royce, to work together to see whether they could collectively lower the costs of certain metals used.

*(*Continued On The Following Page)*

As part of those efforts, members of the consortium shared technical data, subject to restrictions on further dissemination. Rolls Royce reviewed the documents found in Long's possession at Newark Liberty Airport and confirmed that it provided the documents to members of the consortium, which included Pratt. Rolls Royce further confirmed that Long was never an employee of Rolls Royce. A review of UTRC computer records indicated that Long had printed the documents while employed at UTRC.

Long was arrested on a federal criminal complaint on Nov. 7, 2014. A review of Long's digital media seized at the time of his arrest revealed voluminous files protected by the International Traffic in Arms Regulations and Export Administration Regulations, and voluminous files proprietary to various U.S. companies. In short, the investigation revealed that Long took his laptop and the UTRC external hard drive with him to China in 2014, at which time there was a substantial body of highly sensitive, proprietary and export controlled materials present on that digital media. UTRC has confirmed that the hard drive that Long unlawfully retained and accessed in China contained not only documents and data from projects on which Long worked while employed at the company but also from projects on which he did not work to which he would have had access. A sentencing date has not been set. Long has been detained since his arrest.

This investigation is being led by the FBI in New Haven in coordination with Homeland Security Investigations in New Haven and Newark; the Defense Criminal Investigative Service in New Haven; the U.S. Air Force's Office of Special Investigations in Boston, Massachusetts; and, the Department of Commerce's Boston Office of Export Enforcement. U.S. Attorney Daly and Acting Assistant Attorney General McCord also thanked the FBI in Newark, Ithaca and Syracuse, New York, the U.S. Customs and Border Protection Service in New York and Newark, and the U.S. Attorney's Offices for the Northern District of New York and the District of New Jersey, for their efforts and assistance in this matter. This case is being prosecuted by Assistant U.S. Attorneys Tracy Lee Dayton and Stephen B. Reynolds of the District of Connecticut, and Trial Attorneys Brian Fleming and Julie Edelstein of the National Security Division's Counterintelligence and Export Control Section.

National Security Division (NSD)
USAO - Connecticut
Department of Justice
Office of Public Affairs

Singapore Man Pleads Guilty to Plot Involving Illegal Exports of Radio Frequency Modules From the U.S. To Iran

Lim Yong Nam, aka Steven Lim, 42, a citizen of Singapore, pleaded guilty today to a federal charge stemming from his role in a conspiracy that allegedly caused thousands of radio frequency modules to be illegally exported from the U.S. to Iran. At least 16 of the components were later found in unexploded improvised explosive devices (IEDs) in Iraq.

The guilty plea was announced by Acting Assistant Attorney General for National Security Mary B. McCord, U.S. Attorney Channing D. Phillips of the District of Columbia, Director Sarah Saldaña of U.S. Immigration and Customs Enforcement (ICE), Executive Assistant Director Michael Steinbach of the FBI's National Security Branch and Under Secretary Eric L. Hirschhorn of the U.S. Department of Commerce.

Lim was extradited earlier this year from Indonesia, where he had been detained since October 2014 in connection with the U.S. request for extradition. He pleaded guilty to a charge of conspiracy to defraud the U.S. by dishonest means. The charge carries a statutory maximum of five years in prison and potential financial penalties. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendant will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors. Under federal sentencing guidelines, the parties have agreed that Lim faces a range of 46 to 57 months in prison and a fine of up to $100,000. Lim remains in custody pending his sentencing, which was scheduled for XX before the Honorable Emmet G. Sullivan.

Lim and others were indicted in the District of Columbia in June of 2010 on charges involving the shipment of radio frequency modules made by a Minnesota-based company. The modules have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs. According to the plea documents filed today, between 2001 and 2007, IEDs were the major source of American combat casualties in Iraq.

*(*Continued On The Following Page)*

In his guilty plea, Lim admitted that between August 2007 and February 2008, he and others caused 6,000 modules to be purchased and illegally exported from the Minnesota-based company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, Lim and others made misrepresentations and false statements to the Minnesota firm that Singapore was the final destination of the goods. At no point in the series of transactions did Lim or any of his co-conspirators inform the company that the modules were destined for Iran. Similarly, according to the statement of offense, Lim and others caused false documents to be filed with the U.S. government, in which they claimed that Singapore was the ultimate destination of the modules. Lim and his co-conspirators were directly aware of the restrictions on sending U.S.-origin goods to Iran.

Shortly after the modules arrived in Singapore, they were kept in storage at a freight forwarding company until being aggregated with other electronic components and shipped to Iran. There is no indication that Lim or any of his co-conspirators ever took physical possession of these modules before they reached Iran or that they were incorporated into another product before being re-exported to Iran. According to the statement of offense, 14 of the 6,000 modules the defendants routed from Minnesota to Iran were later recovered in Iraq, where the modules were being used as part of IED remote detonation systems.

This investigation was jointly conducted by ICE Homeland Security Investigations (HSI) Special Agents in Boston and Los Angeles; FBI agents in Minneapolis; and Department of Commerce, Bureau of Industry and Security agents in Chicago and Boston. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, the Justice Department Attaché in the Philippines and the FBI and HSI Attachés in Singapore and Jakarta.

U.S. law enforcement authorities thanked the governments of Singapore and Indonesia for the substantial assistance that was provided in the investigation of this matter.

The prosecution is being handled by Assistant U.S. Attorney Ari Redbord of the District of Columbia and Trial Attorney Julie Edelstein of the National Security Division's Counterintelligence and Export Control Section.

Textron Begins On-Water Testing for CUSV

Textron Systems Unmanned Systems, a Textron Inc. (NYSE:TXT) business, announced today that it began on-water testing for the fourth-generation Common Unmanned Surface Vehicle (CUSV™), supporting the U.S. Navy's Unmanned Influence Sweep System (UISS) program.

Textron Systems completed the design, build and component test phases of the UISS program in November 2016. Following component testing, Textron Systems began the systems level integration and test (I&T) phase, culminating in dockside and on-water testing in Lake Pontchartrain near its Marine & Land Systems facility in Louisiana. The I&T phase includes functional testing of the system's integrated generators, engines, datalinks, as well as on-water maneuverability testing. Textron Systems will move into builders' trials upon completion of I&T and then formal testing to validate system functionality with the U.S. Navy later this year.

Web Notice: The Directorate of Defense Trade Controls (DDTC) is currently in the process of modernizing its IT systems. During this time period, we anticipate there may be delays in response times and time to resolve IT related incidents and requests. We apologize for any inconvenience, and appreciate your patience while we work to improve DDTC services. If you need assistance, please contact the DDTC Service Desk at (202) 663-2838, or email at DtradeHelpDesk@state.gov (06.28.16)