



PwC Weekly Security Report



This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.



Risk management

NIST releases Baldrige-based tool for cybersecurity excellence

Encryption

Google, Apple are about to face India's security demands

Threats and vulnerabilities

Schneider power meter issue

Rockwell clears parser buffer overflow

Top story

Cyber hackers publish medical data for Farah, Nadal and Rose

Vladimir Putin accuses Wada of hypocrisy after Olympic athletes' data leak

Volkswagen sets up cyber security firm with ex-Israeli spy chief

Hackers hijack Tesla Model S from afar, while the cars are moving



NIST releases Baldrige-based tool for cybersecurity excellence



The U.S. Commerce Department's National Institute of Standards and Technology (NIST) released today the draft Baldrige Cybersecurity Excellence Builder, a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts.

NIST is requesting public comments on the draft document, which blends the best of two globally recognized and widely used NIST resources: the organizational performance evaluation strategies from the Baldrige Performance Excellence Program and the risk management mechanisms of the Cybersecurity Framework.

Deputy Secretary of Commerce Bruce Andrews announced the release of the draft document today during his remarks at the Internet Security Alliance's 15th Anniversary Conference in Washington, D.C.

"The Baldrige Cybersecurity Excellence Builder answers a call from many organizations to provide a way for them to measure how effectively they are using the Cybersecurity Framework," Andrews said. "The Builder will strengthen the already powerful Cybersecurity Framework so that organizations can better manage their cybersecurity risks."

Using the Builder, organizations of all sizes and types can:

- determine cybersecurity-related activities that are important to business strategy and the delivery of critical services;
- prioritize investments in managing cybersecurity risk;
- assess the effectiveness and efficiency in using cybersecurity standards, guidelines and practices;
- assess their cybersecurity results; and
- identify priorities for improvement.

The Cybersecurity Framework, released in February 2014, was developed by NIST through a collaborative process involving industry, academia and government agencies

NIST was directed by an executive order to create the framework specifically for managing cybersecurity risks related to critical infrastructure, but a broad array of public and private sector organizations now use it. The framework provides a risk-based approach for cybersecurity through five core functions—identify, protect, detect, respond and recovery.

According to a report by the information technology research company Gartner, the framework is currently used by 30 percent of U.S. organizations, a number expected to rise to 50 percent by 2020.

The Baldrige Performance Excellence Program, through its Baldrige Excellence Framework, has helped thousands of organizations worldwide guide their operations, improve performance and get sustainable results for nearly 30 years. It encourages a proven systems thinking approach to achieving organization-wide excellence, driving process improvement and performance management into all key aspects of the organization.

A 2011 economic report estimated the benefit-to-cost ratio of the Baldrige Program to the U.S. economy at 820 to 1.

The Cybersecurity Framework gives order and structure to today's multiple approaches for cybersecurity management by assembling standards, guidelines and practices that are working effectively in many organizations. Applying Baldrige principles enables organizations to maximize the framework's value and manage all areas affected by cybersecurity as a unified whole.

Like the Cybersecurity Framework, the Baldrige Cybersecurity Excellence Builder is not a "one-size-fits-all" tool for dealing with cybersecurity risks. It is adaptable to meet an organization's specific needs, goals, capabilities and environments.

The Builder guides users through a process that details their organization's distinctive characteristics and strategic situations related to cybersecurity. Then, a series of questions helps define the organization's current approaches to cybersecurity in the areas of leadership, strategy, customers, workforce and operations, as well as the results achieved with them.





NIST releases Baldrige-based tool for cybersecurity excellence



Finally, an assessment rubric lets users determine their organization's cybersecurity maturity level—classified as “reactive,” “early,” “mature,” or “role model.” The completed evaluation can then lead to an action plan to upgrade cybersecurity practices and management, implement those improvements, and measure the progress and effectiveness of the process. Designed to be a key part of an organization's continuous improvement efforts, the Builder should be used periodically to maintain the highest possible level of cybersecurity readiness.

The draft Baldrige Cybersecurity Excellence Builder was developed through a collaboration between NIST and the Office of Management and Budget's Office of Electronic Government and Information Technology, with input from private sector representatives.

Public comments on the draft will be accepted until Thursday, Dec. 15, 2016, via e-mail to baldrigecybersecurity@nist.gov.

As a non-regulatory agency of the Commerce Department, NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. For more information, visit www.nist.gov.

Source:

<https://www.nist.gov/news-events/news/2016/09/nist-releases-baldrige-based-tool-cybersecurity-excellence>

Our perspective

The NIST Cybersecurity Framework consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritised, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to manage cyber security-related risks. The self-assessment tool (draft edition) has been created to help organisations better understand the effectiveness of their cyber security risk management efforts.





Google, Apple are about to face India's security demands



India's relationship with the global tech industry has become increasingly fraught. This year alone, the government has banned Facebook's free web service and declined to exempt Apple from local sourcing rules and open its own stores. Now India could force companies to use technology cooked up in a government-funded lab.

The initiative is part of a national biometric identity program called Aadhaar (Hindi for foundation). Millions of Indians use fingerprint and iris-scan authentication to access a range of public and private services that now includes banking. Failure to join the effort could limit the tech industry's access to a vast and growing market, but companies like Apple and Google are expected to resist opening up their phones and operating systems to the Indian registration, encryption and security technology.

"There will be lots of pushing and shoving by the technology companies," says Neeraj Aggarwal, managing director of the Boston Consulting Group in India. "It will be a battle of ecosystems, and companies will do their best to hold on to their own."

A few weeks ago, government officials invited executives from Apple Inc., Microsoft Corp., Samsung Electronics Co. and Alphabet Inc.'s Google to a meeting to discuss embedding Aadhaar encryption into their technology. None of the companies will comment on what transpired at the gathering -- and Apple didn't show up at all.

Ajay Bhushan Pandey, who runs the Unique Identification Authority of India and convened the meeting, says the industry representatives listened politely and were non-committal. But Pandey says he was frank about the government's position, telling his visitors: "Go to your headquarters and work this out so that we can have Aadhaar-registered devices."

India's biometric identity program is something of a path breaker. While the Federal Bureau of Investigation and U.S. VISIT visa program use similar technology to respectively track criminals and foreign visitors, no other country has taken the concept as far as India.

In September of 2010, it began collecting citizens' biometric and demographic data, storing them in a centralized database and issuing a unique 12-digit ID number to every man, woman and child. Aadhaar is the world's largest such program; as of April this year more than one billion people had signed up, or about 83 percent of the population.

Designed in part to help thwart criminals who siphon off billions of dollars in welfare payments each year, Aadhaar helps authenticate millions of poor citizens so the government can send money in lieu of food, fuel and fertilizer subsidies, as well as pension and guaranteed work payments directly to their bank accounts electronically.

Civil liberties and citizens' groups say the program violates Indians' privacy; others warn that Aadhaar's servers could be hacked and compromise national security. But the government is moving ahead and in recent weeks has rolled out a digital payments infrastructure built on top of the program. The idea is to bring financial services to a nation where millions have never set foot inside a bank, let alone opened an account.

As India's billion-user Aadhaar jigsaw fits into place, the government plans to ramp up and add a host of other services including education and health care.

"We are doing 5 million authentications daily, and with Aadhaar-compliant devices that number will grow exponentially," Pandey says. "There is a solid business case for technology companies to enable Aadhaar services."

Indians would still log into their smartphones using the manufacturer's biometric authentication -- typically a fingerprint or iris scan. But once they access Aadhaar using the government's encryption, the likes of Apple and Google would lose the ability to track users online, forfeiting the ability to mine that data to sell ads or other products and services. (Indian law, by the way, bars the government from collecting or using customer data.)





Google, Apple are about to face India's security demands



Tech companies will probably also object to allowing the government to install its authentication software on their gadgets for fear of security breaches and hacking attacks. Apple has strenuously resisted the U.S. government's demands to build a back door into its operating system so law enforcement can track the movements of terrorists and criminals. "There should be clarity and provisions about security," says Amresh Nandan, a research director at Gartner Inc.

On the other hand, foreign tech companies could be at a competitive disadvantage if they don't go along because Indian companies like Flipkart, Paytm and Snapdeal are already making their digital payments and services compatible with Aadhaar. "Once the Aadhaar system grows to scale, technology companies will find it tricky to prevent people from using it," Aggarwal says.

Samsung is the only global device-maker currently making an Aadhaar-friendly device, a tablet that's reportedly selling well. Microsoft is said to be working with the government to link Skype with the Aadhaar database so the video calling service can be used to make authenticated calls. Fresh from battles with Washington over encryption, Apple, Google and other U.S. tech companies are less likely to compromise without a fight.

For now, Indian authorities are asking politely. That could change. Earlier this year New Delhi mandated that, starting in 2017, all mobile phones sold in India must have a panic button women can push when attacked. Nandan Nilekani, who co-founded the leading tech services firm Infosys Ltd. and helped create the national authentication program, says the government could do exactly the same with Aadhaar.

Source:

<http://www.bloomberg.com/news/articles/2016-09-13/india-wants-apple-and-google-phones-to-use-government-encryption>





Schneider power meter issue

There is a public report of a cross site request forgery (CSRF) vulnerability with proof-of-concept (PoC) exploit code affecting Schneider Electric's ION Power Meter products, according to a report with ICS-CERT.

Exploitation of this remotely exploitable vulnerability can allow unauthorized actions on the device, such as configuration parameter changes and saving modified configuration.

The report released while ICS-CERT was working with Schneider Electric to mitigate the vulnerability.

Schneider Electric reports the vulnerability affects the following products: ION 73xx, ION 75xx, ION 76xx, ION 8650, ION 8800, and PM5xxx.

Schneider Electric identified mitigations for this and other issues and will notify their customers. ICS-CERT issuing an alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

ION Power Meter products see use in energy management applications such as feeder monitoring and sub-metering. They interface with power monitoring software or other energy management or automation systems for real-time information for monitoring and analysis.

Schneider Electric also said these devices do not force a change of password upon installation of the device. This is not a vulnerability but a deployment issue. ICS-CERT and Schneider Electric recommend users of these devices (or any other control system device) change passwords from the default settings upon installation of the product.

Schneider Electric offers the following mitigation device:

- Configuration parameter changes, as well as saving modified configuration can be prevented for a meter by setting the "Webserver Config Access" register to "Disabled." This register determines whether you can configure your meter through a browser. Valid entries are Enable or Disable. This register is set to Enable by default.

- There is also an "Enable Webserver" register. This register enables or disables the webserver entirely. Values for this register are YES and NO. The webserver is enabled by default (the value is set to YES).

Some power meters may be revenue locked, which further protects unauthorized meter configuration parameter changes, except Owner, Tag1 and Tag2 string registers

Source:

<http://www.isssource.com/schneider-power-meter-issue/>





Rockwell clears parser buffer overflow



Rockwell Automation patched a parser buffer overflow vulnerability in its RSLogix Starter Lite, then upon further investigation found, and fixed, the issue in its RSLogix 500 and other versions of RSLogix Micro, according to a report with ICS-CERT.

A successful attack may potentially allow malicious code to execute on the target computer at the same privilege level as the logged-in user. The impact to the user's environment is highly dependent on the type of malicious code included in the attack and the mitigations the user may already employ.

Rockwell Automation reports that the vulnerability, discovered by Ariele Caltabiano (kimiya) working with Trend Micro's Zero Day Initiative (ZDI) affects the following products:

- RSLogix Micro Starter Lite, all versions
- RSLogix Micro Developer, all versions
- RSLogix 500 Starter Edition, all versions
- RSLogix 500 Standard Edition, all versions
- RSLogix 500 Professional Edition, all versions

Milwaukee, WI-based Rockwell Automation provides industrial automation control and information products worldwide across a wide range of industries.

The affected products, RSLogix 500 and RSLogix Micro, are design and configuration software used with certain Rockwell Automation products. The software is for use in systems deployed across several sectors, including chemical, critical manufacturing, food and agriculture, and water and wastewater systems. Rockwell said this product sees use on a worldwide basis.

The discovered vulnerability exists in the code that opens and parses the RSLogix 500 and RSLogix Micro project files with an RSS extension.

In order for attackers to exploit this vulnerability in RSLogix 500 and RSLogix Micro, they must create a malicious RSS file.

The buffer overflow condition ends up exploited if an affected version of the product opens a malicious project file. If the attack is successful, the malicious code will run at the same privilege level as the user logged into the machine.

CVE-2016-5814 is the case number assigned to this vulnerability, which has a CVSS v3 base score of 8.6.

This vulnerability is not exploitable remotely and cannot end up exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed RSS file.

No known public exploits specifically target this vulnerability.

Crafting a working exploit for this vulnerability would be easy. An exploit would require social engineering to convince the user to accept the malformed RSS file. Additional user interaction is needed to load the malformed file. This decreases the likelihood of a successful exploit.

Rockwell recommends the following precautionary measures as additional risk mitigation strategies for this type of attack. If possible, employ multiple strategies simultaneously:

- Users using affected versions of RSLogix 500 and RSLogix Micro are encouraged to apply the patch that addresses associated risk and includes added improvements to further harden the software and enhance its resilience against similar malicious attacks. RSLogix Micro version 8.40.00 or RSLogix 500 version 8.40.00: Apply patch KB878490, which can be found on Rockwell's web site.
- Do not open untrusted RSS files with RSLogix 500 and RSLogix Micro.
- Run all software as user, not as an administrator to minimize the impact of malicious code on the infected system.
- Use trusted software, software patches, and anti-virus/anti-malware programs, and interact only with trusted web sites and attachments.





Rockwell clears parser buffer overflow

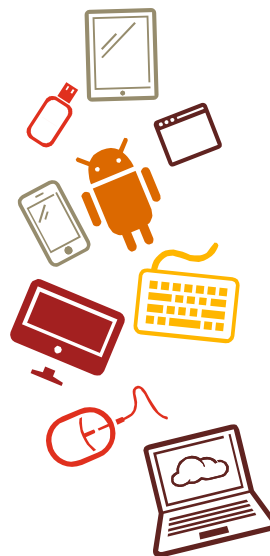


Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.

- Use of Microsoft AppLocker or other similar whitelisting application can help mitigate risk. Click here for information on using AppLocker with Rockwell products.
- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing VPNs may have vulnerabilities and should end up updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

Source:

<http://www.isssource.com/rockwell-clears-parser-buffer-overflow/>





Cyber hackers publish medical data for Farah, Nadal and Rose



Olympic champions Mo Farah, Rafael Nadal and Justin Rose were among athletes targeted on Monday in the latest leak of confidential medical documents that the world anti-doping agency (WADA) says were hacked by a Russian cyber espionage group.

Britain's Farah became only the second man to retain the 5,000 and 10,000 metres Olympic titles at the Rio de Janeiro Games last month while compatriot Rose won the first gold medal in golf for 112 years.

Spaniard Nadal, a 14-times tennis grand slam winner, won Olympic men's doubles gold with Marc Lopez. He also won the men's singles title at the 2008 Beijing Games but missed London 2012 due to a knee injury.

WADA has said it believes the hackers, named as APT28 and Fancy Bears, gained access to its anti-doping administration and management system (ADAMS) via an IOC-created account for the Rio Games.

Documents relating to Farah, and published on the fancybear.net website, showed that the distance runner had no active Therapeutic Use Exemptions (TUEs) at the time of the Olympics.

He received intravenous infusions of saline solution, morphine sulphate and vicodin administered orally during a period in hospital between July 3-5, 2014 when he had collapsed after a training run.

Prior to that, he was given a TUE for an 80mg dosage of the corticosteroid triamcinolone in October 2008.

Rose had authorisation for daily dosages of the anti-inflammatory drug prednisolone between May this year and June 20.

The documents relating to Nadal, who was out for more than two months with a wrist injury that forced him to miss the French Open and Wimbledon before the Olympics, showed exemptions in 2009 and 2012.

The fourth release of data so far concerned 26 athletes from Argentina, Belgium, Burundi, Canada, Denmark, France, Britain, Hungary, Spain and the United States.

Other high-profile names included Burundi's Francine Niyonsaba, British cyclist Callum Skinner and double Olympic rowing gold medallist Helen Glover.

TUEs allow athletes to take banned substances for verified medical needs and there is no suggestion any of those named have broken any rules.

WADA has said the "criminal attack" has recklessly exposed personal data in an attempt to smear reputations.

The agency has also said it believes the attacks are being carried out as retaliation for investigations that exposed state-sponsored doping in Russia.

Fancy Bear has previously posted data for U.S. athletes Simone Biles, Elena Delle Donne, and Serena and Venus Williams as well as Tour de France-winning British cyclists Bradley Wiggins and Chris Froome.

Source:

<http://in.reuters.com/article/sport-wada-cyber-idINKCN11P1NQ>





Vladimir Putin accuses Wada of hypocrisy after Olympic athletes' data leak

President Vladimir Putin says the hack of Olympic athletes' data has cast a spotlight on a "hypocritical" decision to bar Russian athletes from the Rio Paralympics.

Putin spoke Monday as the hackers' group known as Fancy Bears, which the World Anti-Doping Agency said was linked to Russia, unloaded another package of Olympic athletes' data. The athletes had permission from sports or anti-doping bodies to use medications that would otherwise be banned.

Putin says that while "we don't approve of the hackers' action, it has helped reveal that people, who took part in the Olympics and looked absolutely healthy, had taken banned medicines giving them an edge in competition."

In contrast, he adds, Russian Paralympic athletes were banned from the Rio Games on a suspicion, a decision he slammed as "dishonest, hypocritical and cowardly."

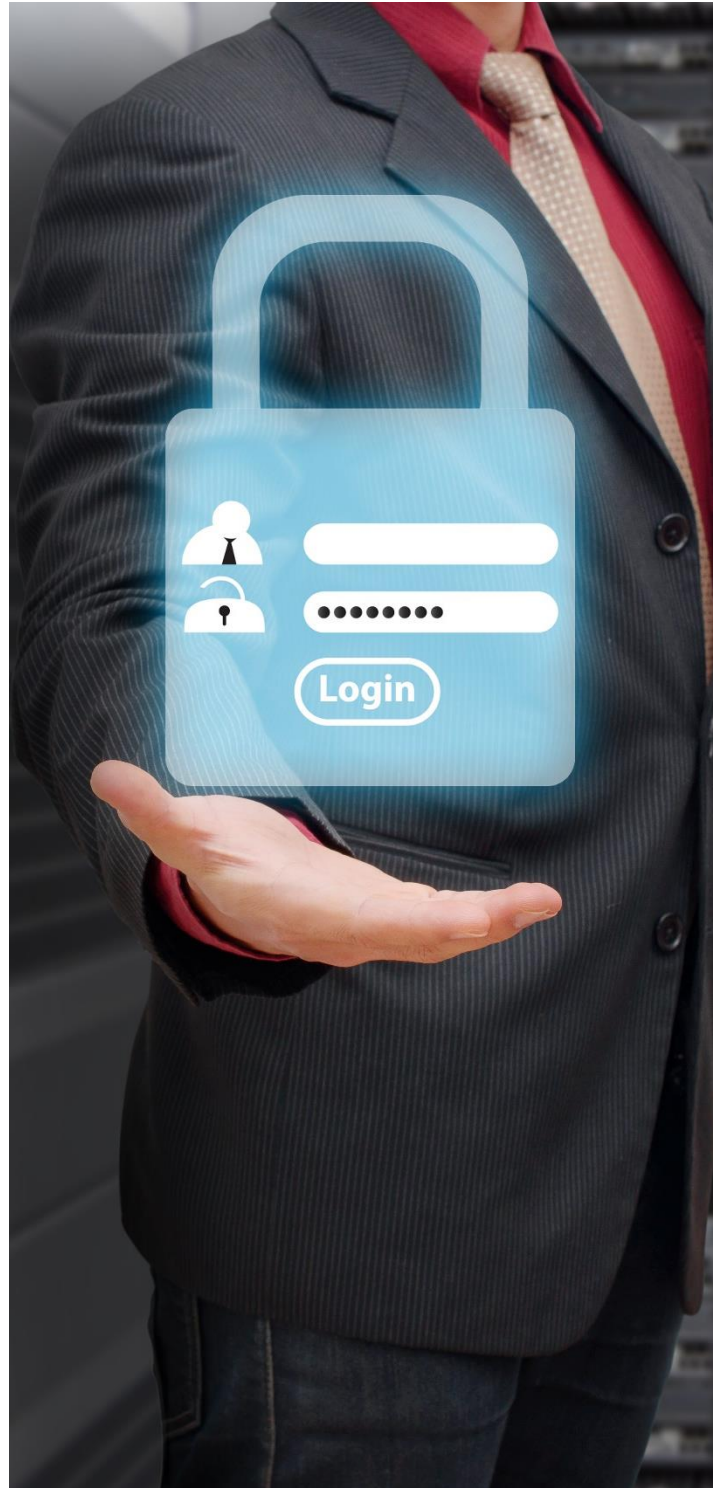
Russia is still smarting after its track and field athletes were banned from the Olympics and its entire Paralympics team turfed out of their Games over evidence of state-sponsored doping.

WADA called the hack "retaliation" after it released reports detailing the cheating and called on Russia to help stop the hacking of its computer systems.

The Kremlin reacted promptly by saying it was ready to help while denying Russian involvement in the hack.

Source:

<http://www.firstpost.com/sports/vladimir-putin-accuses-wada-of-hypocrisy-after-olympic-athletes-data-leak-3011812.html>





Volkswagen sets up cyber security firm with ex-Israeli spy chief

Volkswagen (VOWG_p.DE) is forming a company with the former head of Israel's Shin Bet intelligence agency to develop cyber security systems for Internet-connected cars and self-driving vehicles, the partners said in a statement on Wednesday.

The new company, CyMotive Technologies, will be 40 percent owned by the German automaker and 60 percent by Yuval Diskin and two former colleagues who also had senior posts in the Shin Bet.

The statement did not say how much Volkswagen would invest in the venture, which has an office in a suburb of Tel Aviv and will also open one in Wolfsburg, Germany.

Building on its expertise in technology, Israel has emerged as a leader in the race to keep cars secure and prevent the nightmare scenario of a hacker commandeering your vehicle.

International groups including Harman International Industries and IBM have already bought local companies or invested in research centers.

"To enable us to tackle the enormous challenges of the next decade, we need to expand our know-how in cyber security in order to systematically advance vehicle cyber security for our customers," said Volkmar Tanneberger, Head of Electrical and Electronic Development at Volkswagen.

Diskin has been consulting on cyber security in the private sector since retiring from the Shin Bet in 2011 and will serve as CyMotive's chairman.

Source:

<http://www.reuters.com/article/us-volkswagen-cyber-israel-idUSKCN11K1DA>



Hackers hijack Tesla Model S from afar, while the cars are moving

Chinese researchers control brakes, lights and mirrors with wireless attack

Chinese hackers have attacked Tesla electric cars from afar, using exploits that can activate brakes, unlock doors, and fold mirrors from up to 20 kilometres (12 miles) away while the cars are in motion.

Keen Security Lab senior researchers Sen Nie, Ling Liu, and Wen Lu, along with director Samuel Lv, demonstrated the hacks against a Tesla Model S P85 and 75D and say their efforts will work on multiple Tesla models.

The Shenzhen, China-based hacking firm has withheld details of the world-first zero day attacks and privately disclosed the flaws to Tesla.

The firm worked on the attack for several months, eventually gaining access to the motor that moves the driver's seat, turning on indicators, opening the car's sunroof and activating window wipers.

Keen Security Lab's attacks also appear to soft-brick the Tesla's touch screen which controls much of the car's functions.

"We are able to fold the side mirrors when drivers are changing lanes," Nie says in the demonstration.

"All attacks are contactless without physically modifying the car."

The team demonstrate the remote attacks by triggering very sudden braking while director Lv's model 75D was in motion at slow speed in a car park. The researchers compromised the Teslas in both parking and driving modes.

Director Lv says this type of research is important as cars become more automated and tech-dependent.

He urged drivers to apply any updates when Tesla makes them available.

Source:

http://www.theregister.co.uk/2016/09/20/tesla_model_s_hijacked_remotely/

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

©2016 PwC. All rights reserved



For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

All images in this presentation are protected by copyright, trademark, patent, trade secret and other intellectual property laws and treaties. Any unauthorised use of these images may violate such laws and shall be punishable under appropriate laws. Our sharing of this presentation along with such protected images with you does not authorise you to copy, republish, frame, link to, download, transmit, modify, adapt, create derivative works based on, rent, lease, loan, sell, assign, distribute, display, perform, license, sub-license or reverse engineer the images. In addition, you should desist from employing any data mining, robots or similar data and/or image gathering and extraction methods in connection with the presentation.

© 2016 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.