TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Uber paid off hackers in massive data breach cover-up

Uber is a company that has been in a PR tailspin for some time now. Between shafting their drivers in payments to the business that the company has siphoned away from traditional cab drivers, the corporation has not had a great public perception. Things weren't helped by a massive data breach that exposed well over 57 million customers and their private data (such as names, email addresses, driver's licenses, and phone numbers) to cybercriminals.

December 2017

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

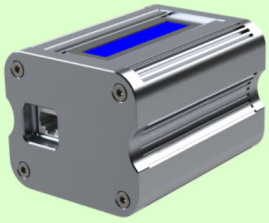
The breach occurred in 2016, but news reports are now emerging that make this story even worse.

As initially reported by Bloomberg's technology news division, it appears that Uber engaged in a massive cover-up of the incident (which was more or less in vain). According to the article, upon first discovering that their private GitHub coding site (which is used by Uber engineers) was compromised, and it became apparent how bad the breach was, Uber tracked down the hackers responsible. In an attempt to keep the breach quiet, Uber upper management paid the hackers $100,000 to delete the data that they had obtained. The hope was that customers would be none the wiser and that the hackers would back off (which is a foolish belief to hold).

This directly flies in the face of protocol for cybersecurity breaches. Per local and federal law, companies are required to report data breaches to the public and government authorities when they occur. Uber had already been on thin ice with numerous prior data breaches, so this cover-up only further hurt any legal standing that the company had. In the aftermath of the revelations the current CEO of Uber, Dara Khosrowshahi (who was not CEO when this occurred), had this to say:

None of this should have happened, and I will not make excuses for it… we are changing the way we do business… At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals… We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.

Latest Network Security Device: "NetDefender"



Vulnerability Management Solution

The new NetDefender Vulnerability Management Solution enhances security by proactively identifying, monitoring, and notifying businesses of potential vulnerabilities in their networks—all with breakthrough simplicity and affordability.

Utilizing proprietary software and the compact NetDefender Sensor, NetDefender works in three phases:

1. Identification

The user's network is continuously scanned to locate and identify every connected device with an IP address, from computers and smartphones to printers and smart devices

Includes scanning of external-facing IPs to provide a 360-degree view of network vulnerabilities

2. Monitoring

All connected devices are then scanned 24x7 for vulnerabilities such as missing software patches

3. Notification

All scan information, including vulnerabilities, is displayed in an easy-to-read dashboard, including instructions for remediation

A proprietary "SPF" (Security Protection Factor) scoring system makes it easy to understand the network's health

Users and their IT security providers can be alerted to critical issues via email or text

For more information on this solution please contact your Tech Hero representative at (800) 900-8234 (option 2)

Khosrowshahi has inherited a significant mess as the new CEO of Uber, but only time will tell if this is the last time the company decides to act as though it is above the law

Client Spotlight

PRIORITY CREDIT UNION

As the name Priority Credit Union suggests, we make satisfying our members a priority. Our tagline, "For Those Who Deliver," gives a nod of recognition to our postal members and heritage but also, as a credit union that is open to the whole community, to our entire family of hard-working people who in their own way "deliver" every day by supporting their families and their community.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

tech hero

ENTERPRISE MOBILE SECURITY: WHY IT MATTERS AND WHAT YOU CAN DO TO ENSURE IT

Back in the days when enterprise mobility was a fascinating reality achievable for only the most advanced enterprises in the world, the most common security concerns centered on network security and data encryption. However, enterprise mobility picked up steam quicker than most estimated, and is now the modern way of work for even small and medium-sized businesses. And with this well-paced adoption of mobile technologies have come unintended consequences: enterprise mobile security woes.

Contemporary enterprise mobile security challenges are complicated, make no mistake about it. Mobile security-related challenges affect businesses in obvious as well as untold ways. So, before anything, let's understand the security challenges that enterprise mobility can pose.

Biggest enterprise mobile security risks for IT to address

IT doesn't have a choice; it needs to address several enterprise mobility-related challenges and risks. Here are a few of them.

- It takes one wrong move to disrupt the fine balance between ease of information access and information security.
- Regulatory and compliance frameworks around mobile data storage are maturing; enterprises need to stay in sync with them.
- Accumulated unencrypted information and flawed inputs can be exposed to other business apps and increase potential threat surface area.
- Mobile infrastructure security evaluation frameworks are expanding, calling for advanced audits, code analyses, and penetration testing; it's challenging for enterprises to quickly adopt these practices.
- Problems resulting out of file sharing and accesses made out of secure networks.
- Issues faced in ensuring that employees use complex passwords for mobile devices they own and use for work.
- Implementing policies and standards across platforms.

A word on mobility management toolkits

From a purely applications-powered perspective, enterprises can begin by using traditional mobile device management toolkits, or adopt more advanced enterprise mobility management (EMM) software. There are also more recent unified endpoint management (UEM) solutions on the shelf for enterprises that heavily rely on mobility solutions.
However, mobility management solutions and frameworks can only deliver their promised benefits if they're backed by strong practices. And that's what we will focus on in this guide.

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-8324 (option 2)

Sales@TechHero.com

Mobile screen projection: First line of defense

Mobile device screen protection is the first line of defense for mobile device protection. The different options for screen protection include PINs, passwords, and patterns. All of these offer a varying level of protection. For instance, traditional four-character PINs can be cracked if the data thief gets 10,000 attempts!

Enterprise IT can use ActiveSync to push screen protection settings on mobile devices within its network. Also, it's possible to use mobile device management software to push security policies on user mobile devices. Unless this first line of defense is bolstered, enterprises can't really hope to thoroughly secure their mobile devices.

Its's also possible to use functionalities such as raising alerts when a specific number of unsuccessful attempts to access a mobile device are made, or to erase device data on suspecting malicious data transfer activities.

Secure mobile Internet browsing

Mobile web browsing to access work email and cloud-based business apps is a reality that all kinds of businesses deal with. Of course, it poses enterprise mobile security challenges. The threats are more real than ever, even more so with the kind of ransomware attacks the world has witnessed in 2017. Here are some best practices:

- Containerized storage areas to separate personal and work-related Internet use on mobile devices.
- Anti-malware protection or mobile devices.
- Training on safe browsing best practices for employees using mobile devices to access work information. Some employees may doing it all wrong! And hopefully, none of them intentionally screw anything up like Vincent Moore did in the excellent movie "Chappie"!
- Use UEM and EMM tools to implement secured file sharing and data sync practices.

Patching and security upgrades for mobile apps and operating systems

To keep mobility infrastructure and endpoints safe and secure from threats and data leakage, enterprise IT needs to implement super-strong practices around patching and system upgrades. This is relevant for mobile applications, as well as all kinds of operating systems used on mobile devices.

Whereas patching has been stressed as the most critical IT security responsibility for enterprise application management, the same thought process needs to be extended to mobile applications and operating systems. If you work with dedicated vendors for mobile apps, it makes sense to have a detailed discussion on the patching and upgrading practices they can help you with.

Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

Identity and access management best practices and applications

Identity and access management needs to encompass mobile devices, along with computers and applications. Mobile access and identity management solutions can deliver massive benefits to enterprises with a large number of mobile apps and mobile devices in its portfolio.

Whether it's about managing access for employees joining or leaving different teams, or about controlling the levels of authorizations of access for employees, this software proves invaluable for businesses in controlling everything related to how an employee is able to use a company-owned mobile device and helps ensure enterprise mobile security.

Do your due diligence

We strongly recommend that enterprises perform thorough mobile security risk assessments before even beginning to attempt implementation of mobility management best practices. Agreed, there are advanced tools that work seamlessly with VPN technologies and Active Directory. However, it's only when IT recognizes the unique risks it faces in terms of mobility that these applications can actually be used to remedy the situation.