TAG-ITI

Talal Abu-Ghazaleh Information Technology International

Newsletter

MARCH 2018 | ISSUE 21

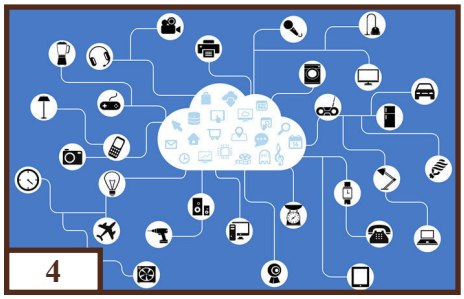
IN THIS ISSUE

1

New beta smartphone application launched by the Arab International Society for Management Technology (AIMICT)

2

A look back at cybersecurity in 2017



4

Where will Microsoft spend $5 Billion on Internet of Things (IoT)?

5

Facebook has lost $80 billion in market value since its data scandal

New beta smartphone application launched by the Arab International Society for Management Technology (AIMICT)

AMMAN- AIMICT has launched it's a beta version of its new mobile application for Android and iOS platform, in order to meet the increasing demand for its services and courses globally

The application is designed to provide users with rich functionality to help them interactively explore the courses offered by AIMICT and take advantage of other services the professional body offers.

Ms. Majd Farahat, AIMICT Executive Director said "The launch of the beta version of the application is the first step in providing users with functionality that has not been previously available. It will provide users with access to the vast amount of services and courses we have to offer through an easy to use, intuitive smartphone application."

She went onto say "The application will eventually feature a mobile learning system which means that users will be able to learn on the go forum anywhere on the globe and will help transform the way the professional education is delivered. This is part of HE Dr. Talal Abu Ghazaleh's vision to help democratize education, making it available to any user, anytime from any device."

The application can be downloaded from the play store/app store, using the keyword 'AIMICT'.

A look back at cybersecurity in 2017

The fact is no enterprise or individual is immune to a breach. What really matters is, did they have an intrusion but then prevent a data loss? Any company can and will likely have an unauthorized intrusion, but did they have the right prevention, detection and response processes in place to stop a loss?

A few years back Gartner reported that prevention is Futile, that we must focus on detection and reaction. This is because there are simply too many ways in to prevent 100% of intrusions.

According to the 2017 Ponemon Cost of Data Breach study, the global average cost of a data breach is $3.62 million. Despite all the new and innovative Tools and Technologies Data Breaches still happen.

As my ISSA colleague Ira Winkler and his coauthor Araceli Treu Gomes point out in their latest book Advanced Persistent Security, most so-called advanced attacks are not really so advanced: “when you look at most of the attacks that have been proclaimed sophisticated by the victims or the consultants who pay to speak for them you see insufficient protection combined with insufficient detection capabilities.”

The top three data breaches of 2017 were:
Equifax, September 7, 2017:
Equifax, one of the three largest credit agencies in the U.S., suffered a breach that may affect 143 million consumers. Due to the sensitivity of data stolen, including Social Security numbers and driver’s license numbers, this is being called one of the worst breaches of all time. Hackers were able to gain access to the company’s system from mid-May to July by exploiting a weak point in website software. The breach was discovered by Equifax on July 29, 2017 and at that time, they sought assistance from an outside forensics firm. Other compromised data is said to include full names, addresses, dates of birth, credit card numbers, and other personal information.

Verizon, July 13, 2017:
A reported 14 million Verizon subscribers may have been affected by a data breach; this may include anyone who contacted Verizon customer service in the past six months. These records were held on a server that was controlled by Israel based Nice Systems. The data breach was discovered by Chris Vickery, who is with the security firm, UpGuard. He informed Verizon of the data exposure in late-June, and it took more than a week to secure the breached data. The actual data that was obtained were log files that became generated when customers of Verizon contacted the company via phone.

Kmart, May 31, 2017:
Sears Holdings, the parent company of Kmart, revealed that Kmart's store payment systems were infected with malware, but Kmart.com and Sears shoppers were not impacted by this breach. The malicious code has been removed, but the company has not shared how long the payment system was under attack and how many stores were affected. No personal identifying information was compromised, but certain credit card numbers may have been.

And on Oct 3, 2017 we learned that Yahoo announced that the huge data breach in August 2013 affected every user on its service — that's all three billion user accounts and up from the initial one billion figure Yahoo initially reported.

These data breach lists always elicit a "gee whiz, that's amazing," response. But what really matters is: Why? Why was there a breach with 1 million or even 100 records? What was the root cause?

I always like to cite the Verizon Data Breach Investigations report which states the following for 2017:

- 75% of breaches were perpetrated by outsiders
- 62% featured hacking
- 81 % leveraged stolen or weak passwords
- 51% included malware
- 24% of the victims were financial institutions
- 66% of malware was distributed via infected email attachments
- 61% of the data breach victims in this year's report are businesses with under 1,000 employees
- 95% of phishing attacks that led to a breach were followed by some sort of software installation

So, computer security is very complex and always involves the human element.

People are the users of all this technology and it's often their daily decisions that can make a big difference. Should I share this file via email without encryption? Should I encrypt this data on my local drive? Is it being backed up? What is the data classification of the data I work with daily? Is that email from a company employee? Why are they asking for this information? Why did they send a Zip or Exe file? All red flags for scammers and cyber criminals.

We know there is no such thing as 100% security but with protective, detective and reaction, you're highly likely to stop the exfiltration of valuable company assets.

https://www.csoonline.com/article/3239405/data-breach/a-look-back-at-cybersecurity-in-2017.html

Where will Microsoft spend $5 Billion on Internet of Things (IoT)?

Microsoft's announcement of $5 billion in new IoT investment is a public demonstration of the company's commitment to the internet of things, but it's not immediately clear what it will spend all that money on.

In a statement announcing the new spending – to be spread out over the next four years – Microsoft cited research from A.T. Kearney that said IoT will bring a nearly $2 trillion productivity increase to the global economy and a $177 billion reduction in business costs by the end of the decade.

There are a lot of use cases for IoT in the enterprise, and Microsoft listed several customer wins in its announcement, including Johnson Controls, Kohler and the Alaska Department of Transportation. Gartner research vice president for AI and IoT Mark Hung said that it's possible to divide those cases into internal and external uses.

Internal IoT deployments might be aimed at optimizing the way a company uses its resources or to improve security and safety for its employees. External ones are more likely to be novel ways of customer engagement – say, location-based services or advertising – or enhancements to customer service, Hung said in an email.

But Microsoft's not offering a lot of guidance on the precise nature of its new spending. Merritt Maxim, principal analyst at Forrester Research.

According to Maxim, Microsoft spent $13 billion on R&D last year, though that wasn't broken out into IoT and non-IoT spending. Nevertheless, he said he suspects that the new money announced today could go toward products and even infrastructure, like giving Azure a bigger worldwide footprint by making it available in more regions.

"The track record on Azure IoT Suite has been pretty good, so I'd view this investment as trying to sustain their position and momentum in the marketplace," said Maxim.

What's more, he noted, it's also a possibility that some of the funds could go toward M&A activity, depending on whether the right companies are out there to be acquired.

"[Especially] if time-to-market concerns become an issue on the whole buy v. build [spectrum]," Maxim said.

https://www.itnews.com/article/3268080/internet-of-things/where-will-microsoft-spend-5b-on-iot.html

Facebook has lost $80 billion in market value since its data scandal

The crisis began on March 16 after Facebook (FB) said it was suspending data analysis company Cambridge Analytica for allegedly harvesting data from more than 50 million Facebook users. Cambridge Analytica worked on Donald Trump's presidential campaign.

Since then, Facebook's stock has plunged 18%, wiping out nearly $80 billion from the social networking giant's market value in the process. Zuckerberg's net worth has fallen by about $14 billion. (He is still worth $61 billion, though).

Tech stocks in general have taken a hit since the Facebook allegations first came to light. The Nasdaq is down 6%.

And other social media companies, most notably YouTube owner Google and Twitter, have both nosedived as well. Shares of Google parent Alphabet (GOOGL) fell 7% since March 16 while Twitter has plunged 20%. Twitter (TWTR) was down 12% alone on Tuesday after noted short seller Citron Research has changed its tune on the company's stock.

Investors worry that Facebook, Google and Twitter could all face tougher regulations in the United States and around the world because of the Cambridge Analytica controversy.

If that happens, it could stymie growth for all three companies -- but Facebook in particular. Investors also worry that users may flee these companies because of privacy concerns. And if users flee, advertisers may eventually jump ship too.

That's why several Wall Street analysts have lowered their price targets and earnings estimates for Facebook during the past week and a half. But others have boosted their forecasts, arguing that the worst will soon pass and that investors are overreacting.

It's impossible to know if it's the Facebook bulls or bears who will ultimately be proven correct. But it's clear that confidence in Facebook and other once-hot tech companies has been shaken.

"While the scandal is likely to blow over, investors should be aware that a continued sell-off in this sector would not be surprising, and if another scandal were to hit, it just might break the tech sector's back," said Craig Birk, executive vice president of portfolio management at investing firm Personal Capital in a note Tuesday.

http://money.cnn.com/2018/03/27/news/companies/facebook-stock-zuckerberg/index.html

For More Information:

Talal Abu-Ghazaleh Information Technology International TAG-ITI

Tel: (0962-6) 5100900
Fax: (0962-6) 5100901

Or you may reach us electronically through our website:
TAGITI.com

And our email:
shalling@tagiti.com

This newsletter is published by:
Talal Abu-Ghazaleh Information Technology International (*TAG-ITI*)