A roving robot Buddy to watch over your home

Reporter: Vrushang Gheewala
Source: www.cnet.com,
Date :September 2015, at 7:00pm
Roll No: A008
Class:SYBscIT

'm a bit torn when it comes to "**The Jetsons**'" vision of the future. Flying **cars**? Count me in. But Rosie, the family's omnipresent robot housekeeper is kind of...meddlesome. I mean, do we really want autonomous busybodies taking control of our homes?

If Paris-based startup Blue Frog Robotics' **Indiegogo campaign** for Buddy -- a "companion robot" designed to help you out with everything from basic reminders to security and even smart gadget control -- is any indication, we really, *really* do.

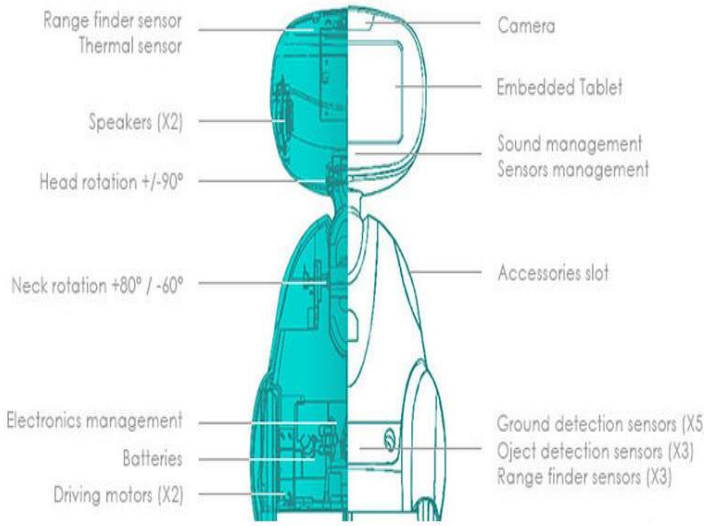
With just hours to go on the Buddy crowdfunding project, backers have contributed over $400,000/£255,000/AU$550,000 toward the promise of a real-life Rosie (well exceeding Blue Frog Robotics' original $100,000 goal.

Weighing in at 11 pounds (5kg) and just shy of 2 feet tall (56cm), Buddy has built-in motorized wheels designed to travel roughly 2 feet per second. And it's supposed to operate autonomously, moving from room to room with a battery life expectancy of up to 10 hours. The team also offers a docking station (sold separately) if

you want Buddy to automatically return to a charging base.

Outfitted with Wi-Fi and Bluetooth tech, Buddy is supposed to be able to tackle all sorts of tasks. It can keep track of your agenda, wake you up in the morning, and act as a teleconferencing portal, a video- and music-streaming device and a home security sentry (via built-in camera).

It's also supposed to work with third-party smart home products like **Parrot Flower Power**, **Nest Learning Thermostat**, **Nest Protect**, **Netatmo Weather Station**, **MyFox Smart Home Security System**,**Lifx LEDs** and others. Companion mobile apps will be available for **Android**, iOS and Windows users, and Buddy was built on an open platform so developers can get in on the action too.

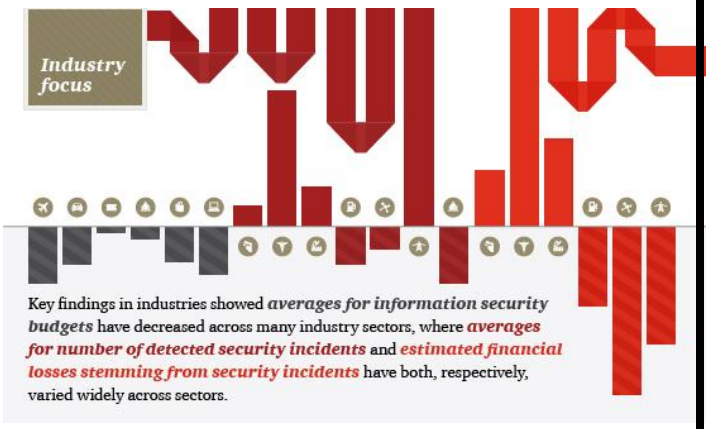


2015 prediction: Expect massive spikes in global information security threats

Source : http://www.techrepublic.com
Reporter: Rajul Hariya
Class: SYBSCIT
Roll No: A010

Global security threats will continue to increase next year and are as certain as death and taxes, according to a recent report.

Increases of global information security threats remain as much a certainty as death and taxes, at least according to the latest Information Security Survey from PWC. That report, which was published in October, highlights several troublesome trends and provides valuable information for those concerned with enterprise IT security. Nonetheless, interpreting the information delivered into applicable best practices remains a challenge for many IT security professionals. Especially those who will be assigned the task of keep their organizations from becoming one of the latest statistics in the battle against cybercrime.



PWC rightly points out that cyber security has become a persistent business risk and that threats (both to the economy and intellectual property) are on the rise. The report goes on to identify some very troubling incidents, including:

- More than half (53%) of global securities exchanges have experienced a cyber attack (IOSCO Survey)
- In South Korea, some 105 million payment card accounts were exposed in a security breach (Symantec Corp)

- City officials in Verden, Germany announced the theft of 18 million email addresses, passwords and other information (TechWeek, Europe)
- Cyber thieves stole more than $45 million from worldwide ATM accounts of two banks in the Middle East (CNet.com)

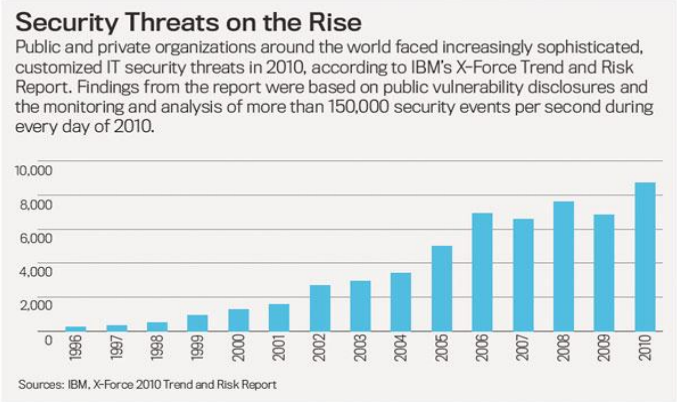
While the above mentioned compromises prove to be just a small fraction of the security incidents that occurred in 2014, those incidents do reveal some of trends, namely that financial gain is a key motivator for attackers and that even the most secure organizations are still susceptible to threats, two realizations that should be game changers for those seeking to protect IT assets from cybercrime.

Is the victim at fault?

When it comes to cybercrime, the complacency of the victims is sometimes at fault. While that does not excuse the criminal nature of the attackers, it does highlight the need for organizations to be proactive in protecting their assets - after all, the law only comes into play after a crime has be committed, meaning that the numerous anti-cybercrime laws on the books hold little sway against determined cybercriminals.

In other words, organizations should be taking a defensive position and grid themselves for attack as inevitability and as not an exception to the rule. That ideology will prove to be a key factor in the paradigm shift needed to protect against the onslaught of attacks expected in 2015.

PwC is forecasting that global security incidents are on track to grow some 48% in 2015, which should strike a dissonant chord with the majority of security professionals.



Is risk management the answer?

With the idea of a security paradigm shift on the table, today's cyber-defenders should be thinking in different terms than just traditional security initiatives, shifting their focus towards an ideology of "cyber risk management", which is being fueled by an initiative founded by the NIST.

The NIST has set forth a security framework (NIST Cybersecurity Framework) that stresses management over technology and highlights several best practices that should help organizations defend against the imminent threats posed by increasing cyber-attacks. While some of the elements of the framework fit under

the realm of accepted best practices and common sense, there are other elements that encompass a sea-change on how organizations deal with cyber threats, namely in the core ideology of five concurrent and continues functions that provide a strategic view into the lifecycle of an organization's management of cyber security risk. Those functions include:

- Identify: Build an institutional understanding of cyber security risk to organizational systems, assets, data and capabilities
- Protect: Develop and implement the appropriate safeguards, prioritized through an organization's risk management process, to ensure delivery of critical IT capabilities without compromises
- Detect: Build the appropriate systems and policies to identify the occurrence of a cyber security event
- Respond: Create and implement the appropriate activities, policies and events that must occur if a cyber-security event occurs
- Recover: Develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cyber security event.

While the NIST states that its methodologies and best practices are optional, the organization does make a strong case for those looking to benefit from a holistic approach to cyber security, and at the very least, sheds some light on what should be an important conversation within any business relying on cyber capabilities to conduct business.

Those charged with the management of enterprise cyber security must delve deeper into what makes up an enterprise's cyber security ideology and make appropriate adjustments before disaster strikes.

3D TECHNOLOGY

REPORTER: DANIEL JACOB
ROLL NO.: A011
CLASS : SYBSCIT

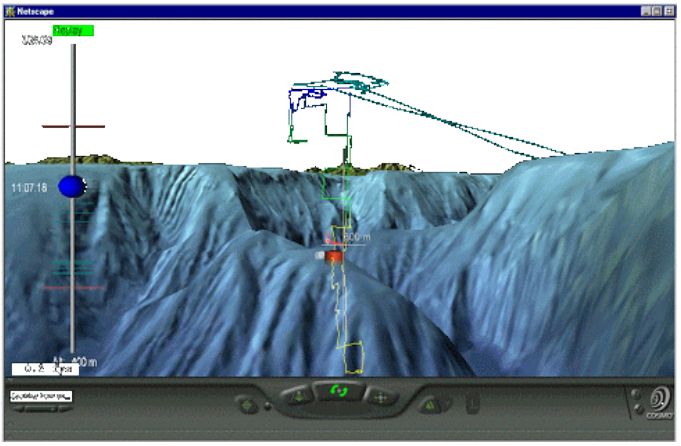
WHAT IS 3D TECHNOLOGY

If you are looking for an informative resource to gain info on 3d technology, then this is the right place for you. The purpose is to offer you in depth information on what is 3D technology, the history as well as the latest technological developments in this field.

In simple words, 3D technology stands for three-dimensional technology that offers a wide array of possibilities in near future in almost every walk of life and especially in entertainment segment. The use of 3d technology in TVs, laptops and other products is growing because the basic content required to support such products includes sports and movies. Lately, the technology has been successful in earning quite a momentum as a valid, widely adopted entertainment technology.

3D technology explained here also points to an important fact that it is not just confined to films being shown in theaters and now the broadcasts made by televisions and direct-to-video films have also started to incorporate similar methods, principally for marketing purposes.

Know more about the application of three-dimensional technology among diverse spheres by explore in the given site. The detailed information featured here would definitely help to sharpen up your knowledge about 3d technology and other useful and



related information to understand the concept of 3D technology.

Nowadays many formats and tools are available, including:

- 3DMLW
- Adobe Shockwave
- Altadyn
- Blend4Web
- Java 3D
- JOGL

- LWJGL
- O3D
- Oak3D
- ShiVa
- Unity
- Virtools
- VRML
- Viewpoint
- Web3D Consortium
- WebGL
- WireFusion
- X3D (extension of VRML)

- Additive Manufacturing File Format

They are mainly distinguished by five criteria:

- Simplicity (Automatic Installation, rates facilities already high)
- Compatibility (Windows, Mac, Unix ..)
- Quality
- Interactivity (Depending on the solutions, their programming opportunities, the creators of content have more or less freedom in the creation of interactivity)
- Standardization

IBM makes push for Linux customers with Ubuntu mainframes

Source: www.zdnet.com,
Date: June 29 2015, at 06:00 pm
Reporter : Darshan Jain
Roll No:A012
Class:SYBscIT

IBM is expanding support for Linux on mainframes with a few new initiatives announced today, including plans for an Ubuntu distribution.
The announcement also includes a new Linux mainframe server called LinuxONE and mainframe code contributions to a new "Open Mainframe Project" formed by the Linux Foundation.

IBM and Canonical are teaming up to create an Ubuntu distribution for LinuxONE and existing z Systems mainframe hardware.

"z Systems clients have enjoyed the performance, security and transactional capabilities of mainframes for decades," Canonical CEO Jane Silber wrote. "By bringing the Ubuntu operating system that developers love to the IBM z Systems mainframe, we will make the cloud and Ubuntu already supports IBM's Power servers, which run Unix and Linux. IBM and Canonical did not say exactly when Ubuntu for mainframes will be available.

There are already SUSE and Red Hat distributions for LinuxONE and z

scale out applications (e.g., Apache Spark, MongoDB, MariaDB, and PostgreSQL) customers love to run on Ubuntu available to the mainframe."

Systems hardware. Though IBM has its own z/OS operating system, it has supported Linux on the mainframe for 15 years.

LinuxONE comes in two sizes for large enterprises and mid-size businesses. The larger one, based on z13 hardware, can "scale up to 8,000 virtual machines or hundreds of thousands of containers—currently the most of any single Linux system," IBM said. SUSE is the first Linux distribution for mainframes to support KVM, a hypervisor for the Linux kernel.

The Linux Foundation's Open Mainframe Project brings together academic, government and corporate members to boost adoption of Linux on mainframes. To get it started, IBM announced a

Though mainframes may seem outdated, they still have a place in many data centers. IBM is hoping to boost adoption with free access to a LinuxONE Developer Cloud that will let developers test and pilot applications without having physical access to a mainframe. IBM said it will also lower the up-front costs of mainframe hardware by offering metered billing for LinuxONE hardware.

issues from turning into failures. The code can be used by developers to build similar sense and respond resiliency capabilities on other systems."

contribution of mainframe code to the open source community, including "IT predictive analytics that constantly monitor for unusual system behavior and help prevent issues from turning into failures. The code can be used by developers to build similar sense and respond resiliency capabilities on other systems."

'We're better off trying to break into Facebook': Engineer who hacked Zomato's 62 million accounts.

Source: Scroll. in Jun 10, 2015 02:30 pm IST

Reporter: Crina Joshi

Class: SYBscIT

Roll No: A013

Hackers feel that Indian startups are often defensive and thankless to engineers who spend days trying to break into their system to expose flaws.

Most often, computer hackers leave a trail of destruction in their wake: defaced websites, stolen credit card numbers, crippled infrastructure. But in recent years, a band of software devotees who call themselves ethical hackers have made valuable behind-the-scenes contributions to keep social media safe for billions of internet users. They have made it their mission to test the security systems of websites and report flaws to the administrators.

These hackers do it for the appreciation and the money that comes with it. As part of its bounty programmes, Facebook doled out an average of $1,343 for 196 bugs exposed by Indian hackers – the most

by any country. One such hacker is Anand Prakash, a security engineer, who hacked popular restaurant discovery and search startup Zomato last week and gained access to 62 million accounts on the site.

Prakash, who works as a security engineer with Flipkart, found that there was a leak in Zomato's database recall system that allowed him to access private information from all the registered accounts by simply replacing his own user id with someone else's. Explaining the drill, he posted the whole procedure, as well as the vulnerabilities in the site's programming, on his blog and even created a video as proof of his access.

Prakash, who had received $12,000 from Facebook for exposing a major security flaw in the website just a few months ago, did not mean any harm. He reported the bug to Zomato's engineering team as well as its CEO Deepinder Goyal and the leak was fixed within a few hours.

"Zomato was very responsive to my emails when I told them about the issue," he told *Scroll*."Facebook had even rewarded me, but Zomato thanked me for this and they fixed it pretty soon so that nobody could take advantage of the same."

Not so receptive

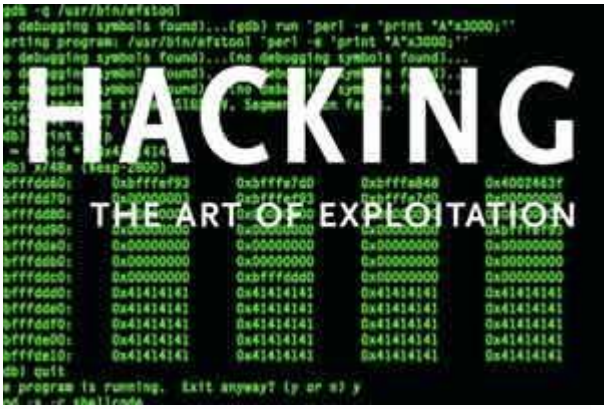
However, all companies aren't so responsive, nor are all hackers so selfless.

Last week, a hacker from Pakistan who goes by the name Mak Man managed to gain access to the huge database of user credentials on the popular music streaming site Gaana.com. Soon enough, the website was down "for maintenance" as he took to the social media to inform people about his act and how he gained access to the database.

Following this, Satyan Gajwani, CEO of Times Internet, the company which runs Gaana.com, commented on this Facebook post and assured Mak Man that the issues flagged by him had been noted and the company would work on fixing it. According to the hacker, he didn't use the user database or keep a copy of it with himself after the fix was applied.

This, however, didn't stop him from complaining about the company's tardy response the last time he had exposed the same flaws. Gajwani had to apologise for this and said, "We've asked Makman if he'd be willing to work with us and help us find any other issues as well."

"I don't think your intention is to expose personal information about Gaana users, but to highlight a vulnerability," he commented on the post. "Consider it highlighted, and we're 100% on it. Can I request that you take down access to the data, and delete it completely?"



Three-minute job?

On the weekend, another hacker claimed that he had gained access to the database of Olacabs, a taxi aggregation platform like Uber. According to a reddit post made by TeamUnknown which claimed responsibility for the act, the hack was tricky but it gave them access to user accounts and unused voucher codes.

“Once we got to the database it was like winning a lottery," the post stated. "It had all the user details along with credit card transaction history and unused vouchers. The voucher codes are not even out yet. It's obvious that we won’t be using credit card details and voucher codes.”

However, TeamUnknown added that they did not plan to use any of the information. “It’s obvious that we won’t be using credit card details and voucher codes,” the post said, and claimed that they had sent an email to the company on this but received no response.

However, Ola claimed that there was “no security lapse whatsoever” and that the hackers had only gained access to one of the model developing platforms which had dummy data used for internal testing. “We confirm that there has been no attempt by the hackers to reach out to us in this regard.”

This is not the first time that people have pointed out Ola’s vulnerabilities. In March, two hackers claimed to have gained access to the transaction system on the app that allowed them to recharge their Ola Wallet accounts by any amounts without paying anything. "All this takes less than three minutes to perform,” one of the hackers told *Business Standard*. The company duly noted the bug this time and fixed it.

Tight purse strings

Stories abound about such hackers who managed to get hired by the likes of Facebook or Google after they were able to access internal database of information after breaching corporate security walls. Prodigies who publicise their work often go on to earn a name for themselves, including job offers and huge bounties from multinationals.

In the past, many such cases have come up where hackers have claimed to breach security of some of the popular Indian tech-startups and posted their modus operandi online, resulting in company taking notice faster than it would through an email.

“It’s easier to grab attention when it’s on a blog or the social media,” said Prakash. “Most companies don’t even respond to hackers when they point out bugs and only some go as far as thanking them for saving them crores of rupees in losses and PR disasters.”

Prakash is not alone. Many hackers have felt that Indian companies are not the best when it comes to acknowledging their security flaws or rewarding those who manage to reveal them. Shubham Paramhans, one of the two people who claimed to have hacked into Ola Wallet, wrote in this blogpost how Ola gave a “very ugly and rude response” when they asked about bug bounty programs.

He further claimed that the company didn’t respond, despite repeated attempts to reach out. According to the post, contacting the CEO didn’t help either as they received nothing but a thanks. “Almost a month-and-a-half month later, I’m still waiting for a reply or an acknowledgement (and I naively thought it was just customer support that sucks at Ola),” he wrote.

Prakash feels that many more people would be inclined to find bugs on Indian startups instead of running to Facebook or Google if they could expect to be appreciated or rewarded. “The rewards motivate people to find bugs, I do this all the time on Facebook because they take quick action and also provide rewards,” he said. “Indian startups are very thankless when it comes to acknowledging someone’s work on their problems.”

Edited by Asiya Shaikh